فصلنامهٔ مطالعات حفاظت و امنیت انتظامی
نشریهٔ علمی (مقاله علمی- پژوهشی)
سال شانزدهم، شمارهٔ پنجاه و هشتم، بهار ۱۴۰۰

تاریخ دریافت: ۱۳۹۹/۱۲/۰۴
تاریخ پذیرش: ۱۴۰۰/۰۱/۲۲

الگوی راهبردی حفاظت اطلاعات آینده در برابر تهدیدهای ترکیبی

محمد عباسی[۱]، حمیدرضا نادی[۲]

چکیده

زمینه و هدف: تهدیدهای جدید از جمله تهدیدهای ترکیبی، کارکرد اصلی اطلاعات؛ یعنی ابهام‌زدایی از تهدیدها را به چالش کشیده است. استفاده‌کنندگان از تهدیدهای ترکیبی برای دست‌یابی به هدف‌های خود، از یک‌سو به طور هم‌زمان از ابزارهای متعدد بهره می‌گیرند تا آثار راهبردی آن را افزایش دهند و از سوی دیگر، کل جامعه را به جای دولت مورد هدف قرار می‌دهند. از این رو بررسی چالش‌های تهدیدهای ترکیبی دغدغه و مسئله نویسندگان مقالهٔ حاضر بوده که در تلاش‌اند تا با هدف ارائه الگوی راهبردی حفاظت اطلاعاتی رافع این مسئله نوین به سهم خود باشند.

روش‌شناسی تحقیق: این تحقیق از انواع تحقیقات کیفی است که با بهره‌گیری از روش موردی- زمینه‌ای انجام شده و اطلاعات لازم به شیوهٔ کتابخانه‌ای و میدانی (مصاحبه با خبرگان) تهیه و داده‌های جمع‌آوری شده با روش داده‌بنیاد، تحلیل و دسته‌بندی گردیده است.

یافته‌ها و نتیجه‌گیری: طراحی الگوی حفاظت اطلاعات سطح راهبردی با سه بعد اصلی ۱. کارکردی که شامل کارکردهای مدیریتی، سیاست‌گذاری، آینده‌نگری و هنجاری؛ ۲. بعد ساختاری حفاظت اطلاعات که مبیین این موضوع است که حفاظت اطلاعات می‌باید ساختاری ملی و دارای جایگاه فراقوه‌ای بوده و ماهیتی غیراجرایی (سیاست‌گذار و نظارت‌کننده و...) داشته باشد؛ ۳. و بعد الزام‌ها و ضرورت‌های حفاظت اطلاعات که در پنج حوزهٔ الزام‌های مربوط به مباحث امنیتی- اطلاعاتی، حفاظت از زیرساخت‌ها و منابع حیاتی، حفاظت از فضای تبادل اطلاعات و امنیت فناوری، حفاظت از اطلاعات بخش خصوصی و الزام‌های مربوط به تهدیدهای ترکیبی است.

کلیدواژه‌ها: اطلاعات، الگوی راهبردی، تهدیدهای ترکیبی، جامعهٔ اطلاعاتی، حفاظت اطلاعات.

---

۱. نویسنده مسئول: عضو هیئت علمی دانشکدهٔ علوم و فنون فارابی (ma10773@gmail.com).
۲. عضو هیئت علمی دانشکده علوم و فنون فارابی (navidali225@gmail.com).

مقدمه

سرعت تغییرها در عصر کنونی که آن‌را گاه عصر ارتباطات و گاه عصر اطلاعات و حتی عصر دانایی می‌نامند به حدی است که تمامی ابعاد زندگانی بشری از فضای زیستی گرفته تا حوزهٔ اندیشه‌ای را تحت تأثیر قرار داده و به‌واسطهٔ این تغییرها، موجودیت و عرصهٔ کنش‌گری تمامی نهادها و سازمان‌ها به درک صحیح و به‌موقع از این دگرگونی و برنامه‌ریزی برای مواجهه با آن گره خورده است. مدیریت نظام امنیتی و حفاظت اطلاعاتی کشور نیز نه‌تنها مستثنا از شرایط این تغییرها نبوده بلکه به عبارتی در نوک پیکان فضای چالش برانگیز عصر کنونی قرار دارد. در چنین محیط و شرایطی، وجود الگویی ساختاری که بتواند علاوه بر شناخت و درک نقاط بحرانی و تهدیدزا و عوامل اثرگذار خارجی و داخلی، با برنامه‌ریزی راهبردی در افق آیندهٔ کنش‌های منفی اثرگذار را که امنیت یک کشور را به خطر می‌اندازد، با کنترل راهبردی مهار کند و متناسب با رخدادهای محیطی و رصد علائم کم‌سو از غافل‌گیری‌های راهبردی پیشگیری کرده و در صورت لزوم و تغییر در مفروض‌های اساسی با تولید راهبردهای مناسب به این رخدادها، واکنش سریع و مقتضی را نشان داده و منافع ملی را در پرتو حفاظت از دارایی‌های ارزشی نظام از اطلاعات گرفته تا اماکن و شخصیت‌ها در افق زمان تأمین کند؛ ضروری به نظر می‌رسد.

با توجه به اینکه نظام جمهوری اسلامی ایران از ابتدا درگیر آسیب‌ها و تهدیدهای متنوع و مستمری از سوی بیگانگان بوده و در طول عمر پُربرکت انقلاب اسلامی، تحت حمله‌ها و فشارهای متعدد امنیتی و اطلاعاتی قرار گرفته است ارائه الگوهایی که بتواند با اقدام‌های عامل و غیرعامل نسبت به خنثی‌سازی این تهدیدها اقدام کرده و بستر

پیشگیری و آموزش عمومی را در موضوع حفاظت از اطلاعات و هدف‌های ارزشمند کشور فراهم کند بی‌شک از راهبردهای اساسی برای مقابله با این تهدیدهاست.

روند متغیرکنونی در عرصه‌های امنیتی و اطلاعاتی و بروز و ظهور تهدیدهای جدید باعث شده تا سطح عملیاتی این تهدیدها اغلب بر پایهٔ اطلاعات شکل گرفته و تکامل یابد و از طرفی گسترش ابزار و فناوری اطلاعاتی و ارتباطی باعث دسترسی و بهره‌گیری عمومی از کالایی به‌نام اطلاعات در وجوه مختلف اجتماعی گردیده و جمع‌آوری آن را از حالت اختصاصی خارج و شرایطی را فراهم کرده است تا آحاد یک جامعه به نوعی هم تولید کنندهٔ اطلاعات و هم مصرف کنندهٔ آن باشند. توسعهٔ اطلاعات پایه، همراه ضرورت حفاظت از ارزش‌های بنیادین کشور، این نیاز را متجلی می‌سازد که چگونه می‌توان از اطلاعات و ارزش‌های نظام در برابر تهدیدهای ترکیبی به خوبی حفاظت کرد؟

از طرفی روبه‌رو شدن با چالش‌های پیچیدهٔ اطلاعاتی و ضداطلاعاتی به‌خصوص در حوزهٔ مسائل قدرت و توسعهٔ ملی، تغییر و رشد فزایندهٔ فناوری ارتباطی و فشار سیاسی و اجتماعی برای آزادسازی اطلاعات به‌طور گسترده‌ای قواعد بازی امنیتی را دستخوش تغییر قرار داده است. از این رو مدیران نظام امنیتی را به جستجوی الگوهای امنیتی و حفاظت اطلاعاتی که متناسب با این نیازها بوده و از ارزش‌های نظام؛ یعنی اسرار، اطلاعات، شخصیت‌ها، هنجارها، اماکن و تأسیسات و ... حفاظت کند، سوق داده است.

بروز تحولات در عرصهٔ ناامنی جهان امروز از یک‌سو و آسیب‌های امنیتی و حفاظتی ناشی از نوآوری‌های جاسوسی و خرابکاری علیه منافع امنیت ملّی در قالب تهدیدهای ترکیبی از سوی دیگر سؤال‌های فراوانی را برای متولیان و مسئولان امنیت و تأمین حفاظت ایجاد می‌کنند از قبیل اینکه آیا ساختارهای موجود حفاظت اطلاعاتی در برابر این مشکلات، آسیب‌های وارده، شیوه‌ها و کارکردهای امروزین می‌توانند موجب حفاظت از منابع و اطلاعات کشور شده و در تأمین و اعتلای عملکرد و کارکردهای حفاظت اطلاعاتی آن مؤثر باشند؟ آیا این کارکرد جوابگوی نیازهای اطلاعاتی و فراهم

کردن زمینه‌های شناسایی، کشف، خنثی‌سازی و مقابله با تعرض رقبا و بیگانگان و برنامه‌ریزی بلندمدت دشمنان برای براندازی یا ضربه‌زدن به منافع امنیت ملی و نظام سیاسی کشورخواهد بود؟

از آنجایی‌که اطلاعات طبقه‌بندی شده و منابع کلیدی نظام جمهوری اسلامی علاوه بر تهدید از طرف سازمان‌های اطلاعاتی دشمن با آسیب‌های متعددی که ناشی از ضعف یا درک‌نکردن یکسان از اهمیت و ارزش حفاظتی آنها در ارکان داخلی کشور مواجه هستند و از طرفی نیز توجه ناکافی به ضرورت حفاظت از زیرساخت‌ها و منابع حیاتی کشور در حوزهٔ غیرنظامی باعث شده تا منافع ملی کشور در معرض آسیب قرار گیرد که برای مقابله با این چالش‌های امنیتی و جلوگیری از درز و افشای اخبار و اطلاعات نیاز است در سطح ملی فرایند و ساختاری را پیش‌بینی کرد تا با نگاهی ملی و با رویکرد جامع و نظام‌مند نسبت به حفاظت از اسرار نظام و سایر ارزش‌های قابل حفاظت اقدام کند.

مقام معظم رهبری(مدظله‌العالی) با درک هوشمندانه از ضرورت نگاه یکپارچه و هماهنگ به موضوع‌های اطلاعاتی و حفاظت اطلاعاتی می‌فرمایند: «دستگاه‌های اطلاعاتی ... باید مثل ظروف مرتبط عمل کنند» (بیانات، ۱۳۸۸/۰۹/۰۸) حفاظت اطلاعات با برقراری ارتباط بین حلقه‌های جدا از هم در حفظ اطلاعات و ظرفیت مهار آسیب‌های ناشی از پراکندگی، خلأ و شکاف موجود در نظام حفاظت اطلاعاتی کشور می‌تواند نظامی هماهنگ و یکپارچه برای حفاظت از اسرار و اطلاعات طبقه‌بندی شده و حفظ موضوع‌های ارزشمند نظام از تعرض و نفوذ نامحرمان و بیگانگان فراهم کند. از این رو بررسی چالش‌های تهدیدهای ترکیبی دغدغه و مسئله نویسندگان مقالهٔ حاضر بوده و در تلاش‌اند تا با ارائه الگوی راهبردی حفاظت اطلاعاتی رافع این مسئله نوین به‌سهم خود باشند.

بدیهی است ارائه الگوی راهبردی ضریب موفقیت و ماندگاری سیاست‌های حفاظت اطلاعاتی را در دنیای رقابتی امروز فراهم می‌سازد، امکان انعطاف و پاسخ‌گویی

هم‌افزا به تغییرهای امنیتی را در اختیار مدیریت نظام امنیتی کشور قرار می‌دهد، امکان موفقیت را متناسب با چالش‌ها و تهدیدهای پیش‌رو و حفظ مزیت‌ها و تأمین قابلیت‌های نوآوری فراهم می‌کند، مدیریت و اشراف راهبردی نظام را متناسب با تهدیدهای ترکیبی ارتقاء می‌بخشد، امکان رقابت، تعارض و مقاومت را شبیه‌سازی کرده و منابع انسانی و تجهیزات و مدیریت فناوری را به‌گونه‌ای توصیه کند که به‌کارگیری روزآمدترین و کارآمدترین شیوه‌ها در حراست از اسرار نظام فراهم آید و اگر در عرصهٔ بروز و ظهور تهدیدهای ترکیبی با آینده‌نگری و آینده‌پژوهی اقدام به‌موقع و مناسب به‌وجود نیاید و جامعهٔ اطلاعاتی از آن غافل بماند ممکن است در زمان لازم انعطاف‌پذیری و ارائه پاسخ لازم و متناسب با تهدید را نداشته باشد و دچار خسران عقب‌ماندگی و پس‌رفت گردد.

پیشینهٔ تحقیق

گری‌گوری.اف.ترورتون[1] در سال ۲۰۰۱ پروژهٔ مطالعاتی تجدید ساختار اطلاعات در عصر اطلاع‌رسانی را به انجام رساندند که در این تحقیق محققان با اشاره به مشکلات و چالش‌های سازمان‌های اطلاعاتی در گذشته که بیشتر بر محور کمبود اطلاعات متمرکز بود به چرخش این چالش به موضوع حجم زیاد اطلاعات و اهمیت‌یافتن تحلیل به جای جمع‌آوری در ساختار و کارکرد جامعهٔ اطلاعاتی پرداخته است.

در پروژهٔ مطالعاتی برترین واقعیت‌های امنیت در عصر اطلاع‌رسانی، بوریس‌دی. برکوویتر[2] و آلن‌ای.گودمن[3] به تبیین تهدیدها و چالش‌های امنیتی آینده برای جوامع جدید پرداخته و این چالش‌ها را در حوزه‌های درگیری‌های قومی و مذهبی و افزایش نقش جهانی سازمان‌های غیردولتی و احتمال بازگشت کشورها به سیاست قرن ۱۹ عنوان کرده‌اند که امروزه هر یک از این موارد مصادیقی از تهدیدهای ترکیبی تلقی می‌شود.

---

1. Gregory.F.Trorton
2. B.D. Berkoviter
3. Allen E Goodman

نهاد ریاست جمهوری آمریکا پروژهٔ مطالعاتی: «راهبرد ملی حفاظت از زیرساخت‌های حیاتی و منابع کلیدی آمریکا» را حمایت کرده و نتیجه آن را به‌صورت سند راهبردی منتشر کرده است. در این سند راهبردهایی برای نهادینه‌کردن مسئولیت حفاظتی و امنیتی اقشار مختلف مردم، صنوف و اتحادیه‌ها و شیوهٔ تعامل آنها با مراکز دولتی ارائه شده است.

دکتر ابراهیم حسن‌بیگی در مقالهٔ علمی «ضرورت حفاظت اطلاعات ملی در بستر تحولات آینده» در سال ۱۳۸۹ به ضرورت درک نقاط بحرانی سازمان‌ها و برنامه‌ریزی راهبردی برای کنترل کنش‌های منفی اثرگذار اجتماعی در آینده پرداخته است. از نظر نویسنده رصد تحولات آینده در حوزهٔ حفاظت اطلاعات، می‌تواند هزینه‌های راهبردی نظام را متناسب با تغییرهای مستمر در حوزهٔ فناوری‌های نوظهور سازگار کند و رویدادها، مخاطرات، ابهام‌ها و تردیدها را مشخص و توانایی انتخاب هوشمندانه را در ارتقای توان امنیت ملی افزایش دهد.

در بررسی جامع ۱۵۵ مقاله از مجموعه مقالات «حفاظت اطلاعات آینده مبتنی بر آموزه‌های دینی و متکی بر روش‌های نوین علمی» که مستخرجه از همایش حفاظت اطلاعات آیندهٔ دانشکدهٔ امام هادی(علیه‌السلام) بوده است مشخص گردید که اکثریت مقالات واصله با در نظر گرفتن یکی از کارویژه‌های حفاظت اطلاعات تلاش کرده نقش فناوری و ابزارهای نوین را در تحول و پیشبرد هدف‌های اطلاعاتی با بهره‌گیری از این ابزارها برجسته کنند. تعدادی از مقالات نیز سعی در تبیین تهدیدهای آینده و نقش حفاظت اطلاعات در مقابله با این تهدیدهای پیش‌رو کرده و نتیجه‌گیری شده که با توجه به چرخش جنگ از حالت سخت به نرم، حفاظت اطلاعات‌های آینده می‌باید نسبت به ارائه راهبردهای مقابله‌ای جدید اقدام کرده و در سیاست‌گذاری‌های امنیتی این موضوع را در صدر اولویت‌ها قرار دهد.

تعریف مفاهیم

الگو: الگو عبارت از کوششی است برای ساده‌تر کردن و آسان‌تر فهماندن واقعیت از طریق تنظیم عناصر و وارد کردن نظم در آنها، به عنوان مثال می‌توان طرح منطقی

روابطی را که بین برخی از عناصر یک سیستم وجود دارد به شکل یک پیکره بیان یا ترسیم کرد (کتولی‌نژاد، ۱۳۹۵: ۲۱).

الگوی راهبردی: الگو پیشرفته‌ای است که با استفاده از آن چیدمان منطقی و هنرمندانه عوامل اصلی، عرصه‌های راهبرد و روابط بین آنها به بهترین شکل ممکن ارائه و مورد بررسی قرار می‌گیرد (حسن‌بیگی، ۱۳۹۰: ۳۴۹).

تهدیدهای ترکیبی: تهدیدهای ترکیبی و جنگ ترکیبی از جمله مفاهیمی هستند که در هزارهٔ جدید برای توصیف چالش‌های امنیتی مورد استفاده قرار گرفته و نمایانگر تغییرها در ماهیت تهدیدها و جنگ هستند و نشان می‌دهند مناقشهٔ قرن ۲۱ بیش از آنکه ماهیت نظامی داشته باشند، حالت ماکیاولی[1] دارند. اصطلاح ترکیبی برای توصیف پدیده‌هایی به‌کار می‌رود که در قالب تعریف متعارف نمی‌گنجند و استفاده از تعاریف سنتی با مشکلاتی مواجه است. تهدیدهای ترکیبی مفهوم وسیعی را دربر می‌گیرد و از این مفهوم برای توصیف راهبرد کلان بازیگران خواهان تغییر وضع موجود استفاده می‌شود که عبارت‌اند از توانایی دشمن در به‌کارگیری اقدام‌های نامتقارن، تسلیحات متعارف، تروریسم و سایر ابزار برای دست‌یابی به هدف‌های سیاسی؛ تهدیدهای ترکیبی بیان‌گر اختلال فزاینده بین سیاست و جنگ در عصر معاصر و تلاش فزاینده برای اخلال در سازمان‌دهی زندگی و روابط اجتماعی به شیوهٔ خاص است. بازیگران تهدیدهای ترکیبی برای دست‌یابی به هدف‌های راهبردیِ خود طیف وسیعی از ابزارها از حمله‌های سایبری تا تبلیغات سیاسی، براندازی، خرابکاری، سیاه‌نمایی اقتصادی و ... را به‌کار می‌گیرند (Monaghan, 2019: 86).

حفاظت اطلاعات و ضداطلاعات: واژهٔ حفاظت در کتب لغت زبان فارسی به معنای حفظ‌کردن چیزی و دفاع‌کردن از آن، مراقبت‌کردن از کسی، چیزی یا جایی و نگه‌داری و مراقبت آمده است (انوری، ۱۳۸۲: ۱۲) حفاظت در اصطلاح عبارت است از همهٔ اقدام‌هایی است که به‌منظور حفظ و نگهداری تأسیسات، اسناد و مدارک، اخبار و

---

۱. در میان انواع تیپ‌های شخصیتی، شخصیت «ماکیاولی» ازجمله رویکردهای منفی به‌شمار می‌رود.

اطلاعات، کارکنان، ارتباطات و سایر موضوع‌های حیاتی کشور در برابر خطرهای ناشی از جاسوسی، براندازی و خرابکاری و سرقت و خطرهای طبیعی به‌عمل آید و از دسترسی افراد غیرمجاز به موارد بالا جلوگیری و ممانعت کند (رستمی، ۱۳۷۸: ۲۳).

حفاظت اطلاعات همهٔ اقدام‌هایی که برای تأمین امنیت و حفظ اطلاعات در قبال تهدیدهایی چون جاسوسی، خرابکاری و براندازی صورت می‌گیرد و از دسترسی عامل غیرمجاز به اطلاعات جلوگیری می‌کند (جمشیدیان و اکبری، ۱۳۹۵: ۹۲).

«Safegard» معادل انگلیسی واژهٔ حفاظت است که علاوه بر حفاظت به معنای تدبیر حفاظتی، اقدام تأمینی، حفاظت‌کردن و محافظت‌کردن آمده است بسیاری از سازمان‌ها حفاظت را معادل اقدام‌های پیشگیرانه می‌دانند؛ یعنی اقدام‌هایی که حوادث و تهدیدها را قبل از وقوع جلوگیری کند (ساحفاناجا، ۱۳۷۸: ۷۱). حفاظت به معنای سلسله اقدام‌هایی است که هدف‌های طبقه‌بندی شده را در برابر تهدیدها تأمین کرده و منجر به افزایش ضریب اطمینان گردد. در معنای دقیق‌تر حفاظت عبارت از کلیه اقدام‌ها، مقررات و قوانین و دستورکارهایی است که به‌کار گرفته می‌شود تا موضوع‌های مهم و حیاتی کشور از دسترس افراد غیرمجاز مصون مانده و از تأثیر فعالیت‌هایی نظیر نفوذ، جاسوسی، خرابکاری، براندازی و خطرهای طبیعی و سهل‌انگاری در امان بماند. (افضل، ۱۳۹۵: ۲۵).

از آنجا که اطلاعات مهم و مرتبط با امنیّت ملّی و نیروهای مسلح همواره مورد نظر دشمن و حریف است و دست‌یابی حریف به آن موجب خسارت و ضربهٔ اساسی و حتی جبران‌ناپذیر می‌شود و از سوی دیگر سامانه‌های مرتبط با اشراف اطلاعاتی مملو از اطلاعات مهم و راهبردی است که مورد توجه دشمن قرار دارد، پرداختن به شگردهای ضدجاسوسی و سایر موارد امنیتی برای ناکام‌گذاشتن حریف در دسترسی به اطلاعات مهم و ضروری است. این مهم در اختیار حفاظت است. شاید اهمیت این بخش از ضداطلاعات از جمع‌آوری اطلاعات از طریق سازمان‌ها مهم‌تر باشد. به همین

جهت، جان لاکر[1]، سازمان اطلاعاتی که مورد نفوذ قرار گرفته را تنها یک سازمانِ بد نمی‌داند، بلکه نقطه‌ضعف هولناکی می‌داند که به جای آنکه چشمی دقیق و بینا برای کشور باشد، گوشی ساده و صدایی گول زننده است که ناآگاهانه مشتریان خود را در حوزهٔ امنیّت ملّی فریب می‌دهد (آستانا و دیگران، ۱۳۹٤: ۹۵-۹٤) در کلی‌ترین تعریف، ضداطلاعات عبارت است از اطلاعات جمع‌آوری و بررسی شده و اقدام‌هایی که به منظور دفاع از یک کشور در مقابل اقدام‌های اطلاعاتی حریف صورت می‌گیرد. طبق این تعریف، گسترهٔ ضداطلاعات به وسعت خود اطلاعات است؛ زیرا باید در مقابل طیف بسیار متنوعی از فعالیت‌های اطلاعاتی حریف دفاع کند. ضداطلاعات عبارت است از ممانعت از دست‌یابی حریف به اطلاعاتی که به او برتری می‌دهد تفاوت بین اقدام غیرعامل و عامل در این است که در اولی سدکردن دسترسیِ (شولسکی، ۱۳۹۲: ۲۱۱) حریف به اطلاعات موردنظر از طریق لایهٔ دفاعی به‌عنوان مثال با کشیدن حصاری به دور آن انجام می‌شود و در واقع یک اقدام تدافعی صورت می‌گیرد، ولی در دومی اقدام‌های تهاجمی و برخورد با فعالیت دشمن نیز مطرح است.

از جمله شیوه‌های تدافعی که تمام قسمت‌های حاوی اطلاعات مهم در سراسر جهان برای کنترل اطلاعات به‌کار می‌برند عبارت‌اند از: طبقه‌بندی اطلاعات، حیطه‌بندی، تعیین صلاحیت افراد برای دسترسی به اطلاعات، نظارت بر دسترسی به اطلاعات و بازیابی اخبار، کنترل حمل و نقل اسناد، نظارت بر چاپ و تکثیر اطلاعات وحفاظت فیزیکی یا قفل و بند مرکز نگهداری اطلاعات (آستانا و دیگران، ۱۳۹٤: ۱۰۸) برای آنکه از الگوی راهبردی اشراف اطلاعاتی برابر اصول و معیارهای حفاظتی، صیانت و حفاظت به عمل آید لازم است در ابتدا مانند هر سازمان دیگر که دارای اطلاعات مهم و محرمانه است اطلاعات دارای اهمیت را به تفکیک میزان اهمیت مشخص و تفکیک کرد تا سقف حفاظت آن بررسی و معلوم شود چه اطلاعاتی باید درحصار قرار گیرد یا چه میزان حصار برای حفاظت آن لازم است.

---

1. J.Laker

در دوران پساجنگ سرد، سازمان‌های اطلاعاتی دچار تحول شدند و این تحول در ضداطلاعات نیز دیده شد که از آن جمله می‌توان به موارد زیر اشاره کرد:

۱) تغییر در طبیعت نقش سازمان‌ها؛

۲) ظهور و بروز تهدیدهای نوپدید در اطلاعات؛

۳) کاهش صبغهٔ جهان‌بینی (ایدئولوژیک) در فعالیت‌های اطلاعاتی در سطح جهان؛

٤) تغییر در روش‌های جمع‌آوری اطلاعات؛

۵) تغییر در طبیعت و ماهیت حریفان و دشمنان اطلاعاتی؛

٦) کاهش ماهیت پنهان‌کاری (عاصم و العیسوی: ۱۳۸۸: ۲٦٦).

در رویکردی دیگر، ضداطلاعات سازمانی است اطلاعاتی و دارای حق بازجویی که اقدام به جلوگیری و خنثی‌کردن فعالیت‌های اطلاعاتی دشمن در داخل و نیروهای مسلح است؛ به عبارت دیگر مسئولیت حفاظت نیروهای مسلح را از نظر جاسوسی، خیانت، خرابکاری، براندازی، تحریکات و نداشتن وفاداری نظامیان بر عهده دارد. (مهدی‌زاده و جوادی، ۱۳۸۷: ٤۱۳) البته برای دستگاه‌های ضداطلاعاتی، شاخص‌های متعدد دیگری نیز بر می‌شمارند که به‌طور نسبی درخور توجه‌اند که از آن جمله می‌توان به اتکا به پشتیبانی قضایی کشور، فعالیت در حوزهٔ سیاسی کشورِ خودی، تمرکز بر اتباع خودی و بهره‌گیری از پوشش در حوزهٔ مأموریتی اشاره کرد (میرجعفری، ۱۳۹۲: ۳۵).

حفاظت رویکردی است که می‌تواند روند حرکت و توسعه قدرت را از آسیب و تهدیدها، ایمن و مصون کند. با حفاظت می‌توان نقاط آسیب‌پذیر را پوشش داد و امکان ضربه و خدشه به هدف‌های مرجع را کاهش داد. در طراحی سازمان‌های ضداطلاعاتی جدید، آمریکا به سه چالش اصلی ضداطلاعات اشاره دارد:

۱) تغییرهای روز به روز فناوری که برای آنها دردسرزا شده است؛

۲) هدف‌های پیش‌رو برای سازمان‌های ضداطلاعاتی نامشخص است؛

۳) فرهنگ سیاسی سخت‌گیرانه، نظام اداری و ذهنیت غلط در ارتباط با ضداطلاعات وجود دارد (سیمس و گربر، ۱۳۹۲: ۳۲۳).

تحولات محیطی و ضرورت حفاظت اطلاعات: علل و عوامل اصلی که ایجاد حفاظت اطلاعات را به اذهان مهندسان نظام امنیتی متبادر می‌سازد طیفی از عوامل امنیتی و اطلاعاتی است که با توجه به تحولات عصر حاضر که تغییرهای فزاینده و شتابگر تمهیدات نو و به‌روزی را دیکته می‌کند باعث شده تا ایجاد حفاظت اطلاعات، راهبردی برای مواجهه با این تحولات در عرصه‌های ذکر شده باشد که به تشریح بخشی از این عوامل پرداخته می‌شود:

۱) **موضوع امنیت:** در گذشته تأمین امنیت فقط بر مفهوم دشمن و تعریف دقیق از آن، در تک‌تک رویدادهای ضدامنیتی، متمرکز بود؛ اما در زمان کنونی، در ادبیات مدیریت امنیت، صحبت از بازیگران و کنش‌گران مرتبط است، چرا که در گذشته، دشمن، مشخص، کم‌شمار و معدود بود ولی اینک در عصر انقلاب اطلاعات و جامعهٔ شبکه‌ای، شمار آنها، به صورت انفجاری رو به افزایش است (برکوویتز و گودمن، ۲۰۰۳: ۲۶-۲۲) همچنین باید توجه داشت که اگر در گذشته، تک‌تک رویدادهای ضدامنیتی، مطرح بودند اینک طیف گسترده‌ای از انواع متفاوت رویدادهای ضدامنیتی واقعی و احتمالی، مدنظر حافظان امنیت قرار گرفته است. در نتیجه نوع نگاه حافظان امنیت و اطلاعات کشور، باید بر رویکرد سیستمی، تمرکز یابد و بر تحلیل تأکید گردد.

۲) **فرهنگ حفاظت و امنیت:** در گذشته نظام حفاظت از اطلاعات به‌صورت عایق‌بندی نظام در برابر هر مخاطره و بحران احتمالی و حمله‌های بالقوه و بالفعل بود. از این رو، سازمان‌های امنیتی کشور، بر پنهان‌سازی، پنهان‌کاری و محرمانگی طیف وسیعی از اطلاعات، تأکید داشتند. در حالی که در وضعیت فعلی حافظان امنیت، شبکه‌سازی، گسترش ارتباطات، شفاف‌سازی و گشایش و گشودگی نظام نسبت به بیرون و انضمام هرچه بیشتر بیرون به درون را تجربه می‌کنند. اساس تغییر در الگوی اطلاعات «باز بودن» است. (ترورتون: ۲۰۰۱: ۳۵۱) در نتیجه مدیریت منابع باز، دیگر اجتناب‌ناپذیر شده است، زیرا که بازبودن و گشودگی، قلب همهٔ دگرگونی‌ها و جابه‌جایی‌ها در فضای چالشی اطلاعات است. برخوردها، درگیری‌ها و مواجهه‌هایی که این دگرگونی عظیم،

برای مدیریت‌های معاصر آفریده است، هم تحلیل داده‌های، متقن و سامانمند اطلاعات امنیتی را مشکل کرده است و هم مسائل و مشکلات مربوط به فرهنگ سازمانی نظام‌های حفاظتی و امنیتی را برای انجام تحلیل‌ها و چگونه تحلیل‌کردن حجم بزرگی از داده‌ها و اطلاعات را مطرح کرده است. در این زمینه، روی آوردن به کانون‌های تفکر غیرمتمرکز، مستقل و اتاق‌های فکر اجتناب‌ناپذیر شده است.

۳) **هدف‌های قابل حفاظت:** در گذشته مدیریت‌های حفاظتی اغلب تعداد محدودی از هدف‌ها (حساسیت‌ها و اسرار) را شناسایی و طبقه‌بندی می‌کردند؛ اما در نظام امنیتی کنونی، این امر به کلی دگرگون شده است چرا که اینک هر نهادی، هر سازمان و هر شرکتی و حتی هر فردی خود را موظف می‌داند، اسرار و حساسیت‌های مربوط به خود را شناسایی کند. در چنین اوضاع و احوالی، مدیریت امنیت اطلاعات دیگر متمرکز نیست و هر مدیریت امنیت اطلاعات منفردی، تنها یکی از ده‌ها و بلکه صدها مدیریتی است که حساسیت‌ها را شناسایی می‌کند. پس آنچه مهم است روحیهٔ همکاری و هماهنگی است. از طرفی با توجه به اینکه خرابکاران آینده شاید حتی کمتر از امروز، دارای سازمان و سلسله مراتب خواهند بود، ولی به‌گونهٔ بهتری با هم ارتباط خواهند داشت. پراکندگی آنان ایشان را ناشناخته‌تر نگاه خواهد داشت اما توانایی آنان در هماهنگ‌ساختن اقدام‌هایی در مقیاس جهانی افزایش خواهد یافت (استراتژی امنیت ملی آمریکا در قرن ۲۱: ۲۰۰۱: ۱۰۳) از این رو هدف‌های قابل حفاظت در معرض تهدیدهای جدیدی قرار خواهد گرفت.

٤) **مدل تولید اطلاعات امنیتی:** در گذشته تولید اطلاعات به صورت خطی بود؛ اما در شرایط جدید به صورت شبکه‌وند؛ یعنی همهٔ منابع تولید اطلاعات، به صورت شبکه به هم مرتبط و متصل‌اند، زیرا فناوری اطلاعات میان آنها وساطت می‌کند؛ به عبارت دیگر هر یک از منابع تولید اطلاعات بی‌شمار، شبکه‌های اجتماعی کوچک و بزرگ و شبکه‌هایی مجازی روی یک یا چند شبکهٔ عمومی یا خصوصی و مجازی قرار دارند. در نتیجه مدل تولید فراورده‌های امنیتی، دیگر به کل عوض شده است به‌طوری که

اطلاعات، مشتری‌گرا و معطوف به نیازهای مشتری، تهیه و تولید می‌شوند، مشتری نیز همان مدیر است که مصرف‌کنندهٔ اطلاعات است. این مشتری در وضعیت قبلی، در آخر خط تولید اطلاعات نشسته بود ولی در پارادایم جدید، جزء شبکه‌وندان است، درست مانند سایر اعضای سازمان امنیتی. پس چنین سازمانی، انعطاف‌پذیر، باز و بر خط[1] است؛ اما آنچه اکنون مهم‌تر شده است، مدیریت چنین سازمان انعطاف‌پذیر و باز است که بسیار پرخطر است و از آن مهم‌تر اعمال نظارت عالیه و حاکمیت بر همهٔ تراکنش‌های بخش اطلاعات است (برکوویتز و گودمن: ۲۰۰۳: ۱۶۹-۱٦٤).

۵) **عرضه و تقاضای اطلاعات امنیتی:** در گذشته که فناوری اطلاعات مطرح نبود و یا کمتر مطرح بود، کارورزی که اطلاعات امنیتی خاصی را کسب کرده بود انگار سنگ بزرگی را به پای خود بسته بود، زیرا اگر می‌خواست آن را به دیگری عرضه کند باید از زور خود برای پیشبرد آن، استفاده کند و آن را با فشار، به جلو براند. مخاطبان اطلاعات امنیتی نیز به میزان وزنه اطلاعات امنیتی، برای اخذ این نوع اطلاعات به همان میزان در مضیقه بودند و گاهی با پافشاری در نپذیرفتن آن و یا هراس در پذیرفتن آن، با اطلاعات امنیتی برخورد می‌کردند، اما امروزه، در عصر انقلاب فناوری اطلاعات، اوضاع بر عکس شده است. مردم برای اطلاعات امنیتی، گوش شنوا دارند، پس به جای آنکه آن را از روی ترس رد کنند با ولع، متقاضی و منتظر دریافت آن هستند، حتی اگر آن را سفارش نداده باشند آن را به سوی خود می‌کشند. در نتیجه، رفتار عرضه کنندهٔ اطلاعات نیز نسبت به سابق، به کل دگرگون شده است: اگر درگذشته، سِمَت، پست، مقام، رتبه و ردهٔ سازمانی عرضه‌کنندهٔ اطلاعات، باعث می‌شد تا اطلاعاتی، از سوی ردهٔ بالاتر جدی گرفته شود، امروزه، آنچه مهم است محتوای اطلاعات امنیتی و شیوه یا چارچوب عرضهٔ آن است و نه سطح عرضه کنندهٔ اطلاعات.

٦) **خصوصی سازی اطلاعات:** در گذشته (و تا حدودی در حال حاضر) بخش امنیت، حراست و حفاظت در انحصار مقامات دولتی بود و یا به‌طور کلی حاکمیتی اداره

1. Online

می‌شد؛ یعنی اطلاعات توسط حاکمیت تولید و از تولید به مصرف حاکمیت می‌رسید؛ اما امروزه به یُمن فناوری اطلاعات، سامانه‌های پشتیبانی تصمیم‌گیری‌های امنیتی، در بخش دولتی، خصوصی به‌کار گرفته می‌شوند و علاوه بر آن، نهادهای پژوهشی متعددی روی کشف و پردازش اطلاعات امنیتی کار می‌کنند. از راهبردهای مهم اطلاعاتی سهیم‌کردن شرکت‌های غیردولتی در اطلاعات و تحلیل است. چون دسترسی بهتری به مراکز تولید اخبار دارند (ترورتون: ۲۰۰۱: ۳۵۹).

۷) **منابع اطلاعاتی:** در گذشته منابع اطلاعات، هر چند سری و پنهانی، باز هم قابل کنترل بودند؛ اما در جامعهٔ شبکه‌ای فعلی، به علت ترکش منابع و انفجار اطلاعات، دیگر نمی‌توان منابع اطلاعاتی را به‌درستی شناسایی کرد و کنترل کرد. پس اگر دیگر نمی‌توان هویت منابع را تشخیص داد، باید بتوان با آنها به شیوه‌ای گزینشی رفتار کرد. در نتیجه، اینک در عصر فجر فناوری اطلاعات روش‌های جدیدی برای گزینش بهینهٔ منابع مطرح شده است. یکی از این روش‌ها رویکرد مدیریت منابع باز است.

۸) **قابلیت دست‌یابی امکانات:** اگر میان دسترسی و دست‌یابی، این تفاوت را قائل شویم که در دسترسی، به صورت بالفعل، منابع و برقراری ارتباط در اختیار متقاضی است؛ اما در دست‌یابی، گرفتن منابع به شکل بالقوه، امکان دارد (مانند دسترسی شخص به کتابی که در کتابخانهٔ شخصی او موجود است و دست‌یابی او به کتابی که در کتابخانه‌ای نگهداری می‌شود و ممکن است اکنون به شخص ثالثی واگذار شده و فعلاً امکان واگذاری به متقاضی جدید وجود نداشته باشد.) پس می‌توان در مورد گذشته گفت: در ایامی که تفکر پنهان‌سازی اطلاعات حاکم بود، اطلاعات، موجود بودند؛ اما دست‌یابی به اطلاعاتی خاص، به تأمین مالی و بر خورداری از صلاحیت، ابزاری خاص و وسایل مکفی نیاز داشت؛ اما امروزه، در عصر فناوری اطلاعات، به جای بایگانی‌های راکد، تفکر استفادهٔ به‌موقع از اطلاعات امنیتی، پویایی لازم را فراهم آورده و اندیشهٔ کاربرد برخط، جای تفکر بایگانی اطلاعات نشسته است. اکنون باید انتظار داشت که مدیریت‌های امنیتی برای خرید تجهیزات سخت‌افزاری و یا تأمین اطلاعات لازم، پول

مورد نیاز را به هر میزان گردآوری کنند، در واقع آنچه فراوان شده است فرصت و اطلاعات است و آنچه دچار کمبود شدید شده است پول و ابزار سخت‌افزاری برای ذخیره‌سازی غیرالکترونیکی اطلاعات است.

۹) **مصرف اطلاعاتی به جای انباشت اطلاعات:** در زمان‌هایی که هنوز فناوری اطلاعات مطرح نبود و یا به بلوغ امروزی نرسیده بود، هزینه‌های گزافی بابت بایگانی اطلاعات طبقه‌بندی شده پرداخت می‌شد؛ اما امروزه، جای جمع‌آوری و ذخیره‌سازی بسیاری از اطلاعات را بررسی و تحلیل اطلاعات گرفته است و چون تحلیل‌گران، اغلب نیروهای انسانی‌اند و حافظه و قدرت تحلیل انسان، جایگاه نخست را دارد، در نتیجه رویکرد مصرف سریع اطلاعات پس از تحلیل یا رویکرد کاربرد، بر رویکرد گردآوری و انباشت اطلاعات خام، غلبه کرده است. علت آن هم این است که فرایند گردآوری اطلاعات، نهایت و غایت ندارد و در تحلیل نهایی، گیج کننده و آزار دهنده است. به همین خاطر سرمایه‌گذاری‌ها، اغلب روی توسعهٔ منابع انسانی متمرکز است. از این رو حفاظت اطلاعات با محیط پویا روبه‌رو است. در این محیط اغلب عوامل اصلی محیط داخلی و خارجی به‌سرعت و به‌شدت تغییر می‌کنند. موفقیت امروز نمی‌تواند موفقیت فردا را تضمین کند؛ بنابراین امروزه نظام حفاظت اطلاعاتی کارآمد و اثربخش خواهد بود که زمان را در اختیار بگیرد؛ به عبارتی دیگر، با آینده‌نگری و پیش‌بینی‌های لازم دربارهٔ تصمیم‌های آینده‌نگری حفاظت اطلاعات خود و همچنین شناخت از کنش‌های منفی و اثرگذار خارجی و داخلی حوزهٔ مدیریتی خود، همواره با برنامه‌ریزی مطلوب واکنش‌های مناسب ر ا پیش‌بینی و طراحی کند.

آینده‌نگاری در حفاظت اطلاعات: آینده‌نگاری همچون پلی می‌تواند گذار مدیریت و نگرش سنتی به پدیدهٔ حفاظت اطلاعات را به رویکردی راهبردی و آینده‌ساز پیوند دهد و این نیازی است که امروز بسیاری از سازمان‌ها برای ارتقای کارآمدی و اثربخشی و پیشگیری از غافل‌گیری احساس می‌کنند تا بتوانند با آینده‌نگری امکان موفقیت خود را در آینده متناسب با چالش‌ها و تهدیدهای پیش‌رو و امکان حفظ مزیت‌ها و تأمین قابلیت‌های نوآوری دنبال کنند.

آینده‌نگاری می‌تواند هزینه‌های راهبردی حفاظت اطلاعاتی را متناسب با تغییرهای مستمر در حوزهٔ فناوری‌های نوظهور سازگار و یا پیشتاز کرده و امکان رقابت، تعارض و مقاومت را شبیه‌سازی کرده و منابع انسانی و تجهیزات و مدیریت فناوری را به‌گونه‌ای توصیه کند که امکان به‌کارگیری روزآمدترین و کارآمدترین شیوه‌ها فراهم آید.

مهندسی هوشمند حفاظت اطلاعات می‌تواند به ممکن‌سازی این آینده یاری رسانده و جوامع مخاطب و هدف را در سازمان حفاظت اطلاعات مدیریت‌پذیر و یا کنترل کرده و ضمن آنکه تصاویری شفاف از سطح تهدید و یا آسیب‌های فراروی آن ترسیم می‌کند امکان شکل‌گیری و جهت‌دهی رفتار مطلوب را در اعضای شبکهٔ حفاظت اطلاعات در حرکت به سمت هدف‌ها و مأموریت‌های آن فراهم سازد (حسن‌بیگی: ۱۳۹۰).

براین اساس مدیریت حفاظت اطلاعات دارای ماهیتی پویاست و پویایی آن به مجموعه اقدام‌های عملی و کنش‌های حرفه‌ای کاربران و مدیران آن مجموعه بستگی دارد که با هدف اشراف و اطمینان از عملکرد حفاظتی و امنیتی در مقابل تهدیدهای حریف و آینده‌نگاری رخدادهایی استوار است که نوید اطمینان در رعایت حفاظت و ایمنی منابع و منافع و فرصت‌های غافل‌گیری حریف را داده و حاکی از احساس امنیت رهبران و کارگزاران در پیگیری هدف‌های ملی است.

در این میان مهم‌ترین اصل در نگاه به آینده، ممانعت از نفوذ رویکردهای ایستا و واپس‌گراست که باید در نگاه مدیران ارشد ملّی مورد توجه و بهبود قرار گیرد. ولی بایسته‌های دیگری نیز در عرصهٔ حفاظت اطلاعات از نگاه پیش‌نگر مورد توجه است که عمده‌ترین آنها عبارت‌اند از (همان: ۱۳۹۰):

- توجه به بروز عوامل یا شاخص‌های پیچیده‌ای که حکایت از جهش‌های فناوری و افزایش سطح مطالبات عمومی مردم و سازمان‌ها در تفسیر از محرمانگی، اطلاعات، سطح دسترسی، حساسیت اطلاعاتی و اقدام پنهان عملیاتی دارد که می‌تواند بسیاری از رفتارهای سوء امنیتی را با موجی از چالش‌های حقوقی و اجتماعی مواجه سازد؛

- توسعهٔ بینش حفاظتی و امنیتی برای مقابله با تهدیدهای نرمی که با تجهیزات شناسایی، امکان کشف و خنثی‌سازی آن در نهادهای حفاظتی اطلاعاتی نبوده و می‌تواند موجب غافل‌گیری راهبردی اساسی گردد، زیرا امروز ظهور تهدیدهای غیرفیزیکی و نرم می‌تواند سازه‌های فرهنگی، جهان‌بینانه، هویتی، وابستگی و وفاداری یک سازمان و یا ملت را به راحتی مورد تهاجم قرار دهد؛
- هرگونه پیش‌نگری و آینده‌نگاری بدون تفکر راهبردی و اصرار بر رعایت اصول راهبردی در مدیریت حفاظت اطلاعات قابل تحقق و تداوم نیست. تفکر راهبردی در این راستا بیش از هر چیز، رویکرد حفاظت و ایمنی ملّی را در بستر هدف‌ها و با جلب مشارکت آگاهانه و تخصصی سازمان‌ها و گروه‌های اجتماعی تلاش دارد تا الزام‌های بنیادین حفاظت از منابع و منافع ملّی را در محیط پُرتلاطم امروزین در قالب توسعه مسئولیت‌پذیری در جامعه مصرف و مخاطب گسترش داده و آنان را برای هرگونه عملیات حفاظتی اثرگذار آماده سازد؛
- عرفی و هنجاری‌کردن حفاظت از اطلاعات، زیرساخت‌ها و منابع حیاتی و بسیاری از ارزش‌های نظام در قالب شبکهٔ جامع حفاظت اطلاعات می‌تواند در کارکردهای حفاظت اطلاعات موجب بهره‌وری و مشارکت فراگیر و توسعهٔ فرهنگ حفاظتی مسئولانه را در کشور نهادینه سازد. همهٔ عناصر این جامعه حفاظتی باید به‌طور یکپارچه و در قالبی هماهنگ با مطالبات حاکمیتی عمل کرده و ابعاد جهان‌بینانه و روانی تهدید را منطبق با استنباط حکومت از تهدید درک و هضم کرده و نقش حمایت‌کنندگی آن را در قالب منافع و هدف‌های امنیت ملّی برعهده بگیرند؛
- مدیریت حفاظت اطلاعات، ترکیبی از دو رویکرد پیوستهٔ مدیریت براساس عقل و حکمت است. توسعهٔ فناوری‌های جدید و جهش‌های حاکم بر افزایش سطح دسترسی، سرعت دسترسی و امکان گزینش، جمع‌آوری و پردازش اطلاعات همچون موجی جذاب تمام سازمان‌ها و مطالبات قدرت ملّی را دربر گرفته است و مدیریت عقلانی توصیه می‌کند تا این عوامل را به‌عنوان مزیت به خدمت گرفته و پرهیز و محروم ماندن از این

کارکرد را موجب انزوا، ناکارآمدی تلقی قلمداد شود. مدیران حفاظت اطلاعات در سطح ملّی باید دو رویکرد عقل و حکمت را با یکدیگر ترکیب کنند و ضمن بهره‌وری از فرصت‌ها، مراقبت و امنیت از منافع امنیت ملّی را تدبیر کنند؛ بنابراین فلسفه و حکمت حفاظتی باید در کنار منفعت اطلاعاتی قرار گرفته و هماهنگ عمل کنند؛

- تجهیز و تقویت دانش در الگوی حفاظت اطلاعات به علوم نرم امنیتی به‌طوری که حساسیت حفاظتی را از حوزهٔ نرم‌افزار تا سخت‌افزار را به دقت پوشش داده و رصد کند. دانش در حفاظت اطلاعات با رویکرد آینده‌نگری باید تقویت کننده و پشتیبانی کننده از محورهای ذیل باشد:

۱) علل و عوامل شکل‌گیری صحنه‌های بروز تهدیدهای نوظهور؛

۲) بررسی و تحلیل عناصر و مراحل ظهور روندهای تعارض، تزاحم و تنازع منافع امنیت ملی و اشکال جدید ناامن‌ساز در حوزه‌های لازم و قابل حفاظت اطلاعات در سطوح ملی؛

۳) کشف و فهم عوامل و اشکال تهاجم اطلاعاتی به منافع حوزه امنیت ملی در سه حوزهٔ نرم، نیمه‌سخت و سخت به‌صورت یک جریان مؤثر و پیشتاز.

توجه به کارویژه‌های تحلیل تحولات محیطی و کلان‌نگر که می‌تواند توان حریف، رقابت و سطح پنهان‌کاری و میزان ترمیم‌پذیری تهدید را مشخص و عامل تغییر را در راهبردهای دشمن مشخص کند.

محیط عملیاتی ضداطلاعات در عصر تهدیدهای ترکیبی: محیط عملیاتی ضداطلاعات در عصر تهدیدهای ترکیبی بسیار تغییر کرده است. قطب‌بندی قدرت‌ها در دوران جنگ سرد سبب شد تهدیدهای اطلاعاتی بیشتر دولت‌محور و دارای ماهیت عینی و به‌خصوص نظامی باشد و سایر کشورها نیز به‌طور مستقیم و غیرمستقیم از این چالش‌های اطلاعاتی متأثر بودند. ما در عصر تهدیدهای ترکیبی با دوران «شبه‌جنگ» مواجهیم که تهدیدهای آن از منابع گوناگون نشئت می‌گیرد و پیش‌بینی‌ناپذیرتر از زمان جنگ سرد است (Cogan, 2004: 165)، دشمن بین بخش خصوصی و دولتی تمایز

قائل نمی‌شود و طیف گسترده‌ای از هدف‌های کم‌خطر را مورد هدف قرار می‌دهد. تهدیدها در این دوره از سه روند نشئت می‌گیرد:

۱) بازیگران غیردولتی خشونت‌طلب که درگیر فعالیت‌های اطلاعاتی تدافعی و تهاجمی هستند و از شبکه‌های ارتباطاتی و مالی خود محافظت می‌کنند؛

۲) بازیگران دولتی دارای توانمندی اطلاعاتی پیشرفته و بازیگران غیردولتی که جنگ ترکیبی را به عنوان راهبرد نظامی- سیاسی خود برگزیدند؛

۳) بازیگران دولتی و غیردولتی و همچنین افراد دارای گرایش‌های جهان‌بینانه به گروه‌های تروریستی (گرگ‌های تنها) که درگیر فعالیت‌های گوناگون از جمله جاسوسی سایبری هستند.

در چنین شرایطی، محیط فعالیت ضداطلاعاتی بسیار متنوع و پراکنده، تهاجمی‌تر شده و به لحاظ فناوری پیچیده و شاید موفقیت‌آمیزتر از گذشته شده است. دولت‌ها و بازیگران غیردولتی با استفاده از ابزارهای گوناگون تهدیدهای ترکیبی در صدد تضعیف دولت هدف و وادارسازی آن به اتخاذ تصمیم‌های راهبردی نادرست هستند که در جهت منافع راهبردی دولت رقیب است و به آنها این امکان را می‌دهد که از این شرایط در جهت هدف‌های خود استفاده کنند.

حوزهٔ سایبری که از آن به عنوان مرزهای جدید تهدیدهای ضداطلاعاتی یاد می‌شود، یکی از حوزه‌هایی است که هم بازیگران دولتی و هم بازیگران غیردولتی از آن برای تأثیرگذاری بر دولت‌ها و جامعه استفاده می‌کنند. فناوری‌های پیشرفته در حال ظهور مانند هوش مصنوعی، رمزنویسی پیشرفته و اینترنت اشیا، ابزارهای ذخیره‌سازی یا جاسازی نرم‌افزارها در درون شبکه‌ها برای استخراج دادها از راه دور، امکان سرقت مقدار زیادی از اطلاعات را افزایش داده است. این پیشرفت‌های فناوری کار ضداطلاعاتی را بسیار پیچیده کرده و دفاع علیه تهدیدهای ضداطلاعاتی را بسیار مشکل کرده است. در حال حاضر، دولت‌ها فضای سایبری را به‌عنوان مکان بسیار مناسبی برای جاسوسی، نفوذ دیپلماتیک، تبلیغات سیاسی، اقدام نظامی و به‌مثابه ابزاری برای اعمال قدرت تلقی می‌کنند.

اتکای دولت‌ها به فضای سایبری برای انجام فعالیت‌های تجاری، اقتصادی و... ، میزان آسیب‌پذیری آنها را در مقابل تهدیدهای سایبری به مقدار زیادی افزایش داده است. این گسترش، سه چالش اساسی را برای افسران ضداطلاعاتی ایجاد کرده است: نخست آنکه آنها باید همهٔ افرادی که همواره با شبکه‌های رایانه‌ای سروکار دارند را مورد بررسی قرار دهند که آیا جاسوس یا افسر اطلاعاتی خارجی هستند که از طریق ابزارهای الکترونیکی، سازمان‌های امنیتی و غیرامنیتی را مورد حمله قرار می‌دهند. دوم اینکه افسران اطلاعاتی باید به قدر کافی در مورد پردازش داده‌ها و شبکه‌های ارتباطاتی آموزش دیده باشند و به‌طور کارآمد با عوامل مدیریت اطلاعات همکاری کنند. سوم اینکه هشدارهای اطلاعاتی را وارد فرهنگ تخصصی مهارت‌های فنی و اطلاعاتی سازند (Redmond, 2010: 554).

نکتهٔ مهم اینکه در عصر تهدیدهای ترکیبی حتی نهادهای اطلاعاتی و امنیتی نیز از این حمله‌ها مصون نیستند. برای مثال، گروه ناشناخته‌ای ابزارهایی که ظاهراً آژانس امنیت ملی آمریکا برای رخنه در رایانه‌ها استفاده می‌کرد را نشت دادند. با نشر غیرمجاز ابزارهای سایبری آمریکا، طیف بسیاری از بازیگران توانستند توانایی پیچیده‌ای را به‌دست آورند که پیش‌تر در اختیار سازمان‌های اطلاعاتی بوده است (Strohm, 2020)؛ علاوه بر این، افشاگری اسنودن نشان داد حتی افرادی که صلاحیت امنیتی آنها توسط نهادهای امنیتی تأیید شده نیز می‌توانند چالش ضداطلاعاتی محسوب شوند.

از سوی دیگر، گسترش وسایل ارتباط ارتباطاتی به‌ویژه رسانه‌های اجتماعیِ اجرای فریب به‌عنوان یکی از ابزارهای اساسی ضداطلاعاتی را آسان‌تر کرده و امکان قابلیت انکار مداخله را افزایش داده است. بازیگران دولتی و غیردولتی این رسانه‌ها را ابزاری بسیار مؤثر و کم‌هزینه برای دست‌یابی به هدف‌های راهبردی خود تلقی می‌کنند و از آن در راستای هدف‌های راهبردی خود برای نفوذ مخفیانه و انتشار اطلاعات نادرست در جامعه استفاده می‌کنند تا از این طریق بر تصمیم‌گیرندگان تأثیر گذاشته یا آنها را فریب دهند، برداشت افکار عمومی را تغییر دهند و تئوری توطئه و بدبینی را در جامعه گسترش

دهند. راهبردهای روسی از آن به‌عنوان تلاش برای کسب برتری خبری و ایجاد شرایطی برای دست‌یابی به هدف‌های خود بدون توسل به نیروی نظامی یاد می‌کنند (McGeehan, 2018: 50).

بازیگران دولتی یا غیردولتی از طریق انتشار اطلاعات نادرست که از آن می‌توان به عنوان براندازی خاموش یا مخفی نام برد، هدف‌های متعددی را دنبال می‌کنند، اما مهم‌ترین هدف آنها تضعیف وحدت و تعمیق شکاف بین بخش‌های مختلف جامعه و کاهش اعتماد بین شهروندان و حاکمان است. آنها تلاش می‌کنند با استفاده از اخبار نادرست عدم قطعیت را افزایش یا با ایجاد قطعیت نادرست افکار عموم جامعه را به نحوی شکل دهند که آنها ناخواسته در راستای هدف‌های دشمنان گام بردارند و تصمیم‌گیران به‌ناچار گرفتار خطای محاسبات راهبردی گردند و سیاست‌ها و اقدام‌هایی اتخاذ کنند که در راستای هدف‌های آنها باشد.

مقابله با تروریسم یکی دیگر از چالش‌های ضداطلاعاتی در تهدیدهای ترکیبی است. مواجه سازمان‌های ضداطلاعاتی با تروریسم اگرچه پدیدهٔ جدیدی نیست؛ اما تروریسم نوین با تروریسم در زمان جنگ سرد تفاوت اساسی دارد. تروریسم در دوران جنگ سرد ملی بوده و اغلب با هدایت و مدیریت قدرت‌های بزرگ قرار داشت و بزرگ‌ترین هدف‌های عملیاتی آنها دولت‌های خارجی و عوامل اطلاعاتی آنها و مقامات سیاسی بود. عمده‌ترین دلیل آنکه ضداطلاعات نقش اساسی در مقابله با آنها ایفا می‌کرد، این بود که آنها اغلب تحت حمایت دولت‌های خارجی قرار داشتند (Bauer, 2016).

در دوران تهدیدهای ترکیبی ما با گروه‌هایی تروریستی مواجهیم که فراملی، غیرمتمرکز و شبکه‌ای هستند. این بازیگران بسیار چابک، انعطاف‌پذیر و انطباق‌پذیر هستند و از فناوری و ابزارهای اطلاعاتی و ضداطلاعاتی پیشرفته‌ای برخوردار هستند. آنها توانمندی اطلاعاتی خود را در زمینهٔ انسانی، فنی و سایبری افزایش دادند و برای تسهیل فعالیت‌های غیرقانونی خود و اجتناب از شناسایی و دستگیری مراقبت‌های فنی انجام می‌دهند (Mobley, 2012: 12-103).

این ویژگی‌ها آنها را قادر به شناسایی آسیب‌پذیری‌ها یا شکاف‌ها در خطوط دفاعی دشمن می‌سازد. این بازیگران همانند دولت‌ها دارای فعالیت‌های اطلاعاتی هستند و به جمع‌آوری و پردازش اطلاعات اقدام می‌کنند. این اطلاعات اغلب راه‌کنشی (تاکتیکی) است و اطلاعات راهبردی در بین آنها ضعیف است. بازیگران غیردولتی از این اطلاعات برای طرح‌ریزی حمله‌های فیزیکی نظامی و حفظ خود از نفوذ و حمله‌های نیروهای دولتی استفاده می‌کنند. ضداطلاعات از نقش بسیار بالایی در این سازمان‌ها برخوردار است و کارآمدی ضداطلاعاتی بقای آنها را تضمین می‌کند. این بازیگران از ضداطلاعات برای حفظ انسجام و وحدت در داخل گروه استفاده می‌کنند. آنها همچنین از عملیات اطلاعاتی برای شکل‌دهی به محیط عملیاتی استفاده می‌کنند و به‌دنبال استفاده از آسیب‌پذیری‌های اطلاعاتی و نفوذ در درون سازمان‌های اطلاعاتی هستند. برای مثال، القاعده در سال ۲۰۰۳ تلاش کرد در نیروهای امنیتی یمن نفوذ کند. نیروهای عملیاتی القاعده در سال ۱۹۹۷ توانستند از دست نیروهای امنیتی قطر فرار کنند. این امر نشان می‌دهد آنها در دولت قطر نفوذ کرده بودند (Gentry, 2015: 10).

الزامات ضداطلاعات در عصر تهدیدهای ترکیبی: در تهدیدهای ترکیبی، بازیگران متنوع هستند و دشمنان با پنهان‌سازی هدف‌ها و نیات خود در صدد گمراهی و فریب تصمیم‌گیرندگان و توده‌های جامعه است و عاملان تهدیدهای ترکیبی از توانایی به چالش‌کشیدن دولت برخوردار هستند. از این رو، ضداطلاعات باید توانمندی خود را در تمام زمینه‌ها تقویت کند. بر این اساس، ضروری است ضداطلاعات شامل سه اقدام باشد:

۱) تبدیل ضداطلاعات به ضداطلاعات راهبردی: در تهدیدهای ترکیبی، هشدارهای حمله بسیار نامحسوس هستند و شناخت فوری آنها امکان‌پذیر نیست؛ به‌ویژه آنکه اقدام‌های این بازیگران بسیار پراکنده و در ظاهر بدون ارتباط به نظر می‌رسند؛ اما در مجموع نمایان‌گر راهبردی کلان هستند. شناسایی و مقابله با آنها نیازمند شناخت بیشتر دشمن و مقاصد و نیات آنهاست و هرچه شناخت بیشتر باشد، امکان موفقیت بیشتر خواهد شد. ضداطلاعات راهبردی، رویکرد مناسب برای شناخت تهدیدها در شرایط کنونی است.

ضداطلاعات راهبردی مبتنی بر سه فرض است: نخست؛ تهدیدهایی که از سوی بازیگران تهدیدهای ترکیبی صورت می‌پذیرد، راهبردی هستند. دوم؛ با تهدیدهای راهبردی نمی‌توان از طریق اقدام‌های موقتی مقابله کرد. سوم؛ تهدیدهای اطلاعاتی راهبردی را باید از طریق پاسخ راهبردی برطرف کرد. هدف از ضداطلاعات راهبردی مواجهه و درگیری با دشمن است. ضداطلاعات ابزاری برای پیشبرد هدف‌ها در سطح راهبردی و حرکت به سمت ضداطلاعات تهاجمی برای تضعیف چالش‌گران و مقابله با توانایی آنها برای اقدام علیه خودی است. در این راهبرد، دولت‌ها باید به‌طور کارآمد از نقطه‌ضعف رقبای خود استفاده کنند و از عملیات‌های ضداطلاعاتی برای ایجاد مزیت‌هایی برای امنیت ملی خود بهره ببرند. در این راهبرد، هدف تنها دستکاری یا ناتوان‌سازی عملیات اطلاعاتی رقبا نیست، بلکه این است که آنها عملیات اطلاعاتی را به‌خوبی انجام ندهند یا اینکه اصلاً نتوانند عملیاتی اطلاعاتی انجام دهند. چنین اقدام‌هایی باید هدف‌های عملیاتی را قبل از اقدام علیه کشور مورد هدف قرار دهد و قبل از اینکه توان بازسازی داشته باشند باید آنها را تضعیف کند. هدف از این عملیات‌ها پیش‌بینی اقدام‌های دشمن و استفاده از این مزیت برای مقابله با آن است.

در ضداطلاعات راهبردی بر ضداطلاعات تهاجمی تأکید می‌شود. برعکس ضداطلاعات تدافعی که مبتنی بر بازدارندگی است، ضداطلاعات تهاجمی مبتنی بر فعالیت‌هایی از قبیل کشف، فریب و خنثی‌سازی است (Prunckun, 2019: 28). در ضداطلاعات تهاجمی سازمان‌های ضداطلاعاتی باید قادر به نفوذ در دستگاه اطلاعاتی دشمن و تأثیرگذاری بر رفتار آنها باشند. سازمان‌های ضداطلاعاتی از طریق نفوذ ضداطلاعاتی می‌توانند به اقدام‌ها و مقاصد دشمنان پی ببرد، اقدام‌های آنها را کنترل کنند و آنها را به سمت تصمیم‌های نادرست هدایت کنند. علاوه بر این، سازمان‌های ضداطلاعاتی از طریق نفوذ می‌توانند ارزیابی راهبردی از توانمندی اطلاعاتی دشمنان خود داشته باشند و با استفاده از این آگاهی، راهبردهای مناسب برای خنثی‌سازی اقدام‌ها و فعالیت‌های آنها تدوین کنند. در چنین حالتی، ضداطلاعات بیش از آنکه

دریافت‌کنندهٔ اطلاعات باشد، به شکارچی اطلاعات تبدیل می‌شود و می‌تواند اطلاعات را شکار کند و قادر می‌شود قبل از وقوع حمله جلوی آن را بگیرد.

۲) ایجاد مرکز هماهنگی جامعه ضداطلاعاتی: مقابله با این تهدیدها نیازمند رویه‌هایی فراتر از رویه‌های متعارف ضداطلاعاتی است. مقابله با این تهدیدها نیازمند راهبرد ضداطلاعاتی است که همهٔ نهادهای جامعهٔ ضداطلاعاتی را دربر گیرد. لازمهٔ این کار ایجاد مرکزی برای هماهنگی فعالیت‌های ضداطلاعاتی بین دستگاه‌های مختلف ضداطلاعاتی است. از همین رو، کمیسیون گزارش ۱۱ سپتامبر اذعان داشت ما در عصر جدید به جای اصل «نیاز به دانستن» به اصل «نیاز به اشتراک» نیازمند هستیم. وجود نهاد جامع ضداطلاعاتی موجب انسجام راهبردی در طیف گسترده از فعالیت‌های ضداطلاعاتی می‌شود. این نهاد با تدوین خط‌مشی و اجرای برنامهٔ ملی موجب هماهنگی در هدف‌های ضداطلاعاتی می‌شود.

هماهنگ‌کردن منابع بخش‌های مختلف جامعهٔ ضداطلاعاتی و تمرکز بر تحلیل تهدیدهای اطلاعاتی و اجرای برنامه‌ریزی راهبردی موجب از بین رفتن شکاف‌ها در جمع‌آوری اطلاعات، تدوین بهترین گزینه‌ها برای کاهش تهدیدها و اجرای هماهنگ اقدام‌ها برای تحقق هدف‌های ضداطلاعاتی تدافعی و تهاجمی خواهد شد. از سوی دیگر، از دوباره‌کاری و اتلاف منابع نیز جلوگیری خواهد کرد.

از این رو، مقابله با این تهدیدها نه‌تنها نیازمند همکاری بین همهٔ نهادهای ضداطلاعاتی در عرصهٔ داخلی است، بلکه نیازمند همکاری‌های ضداطلاعاتی با کشورهای مختلف به‌ویژه کشورهایی است که با تهدیدهای مشترک مواجه هستند؛ چراکه هیچ سازمانی همه چیز را نمی‌داند و نمی‌تواند هر کاری را انجام دهد. همکاری با سازمان‌های ضداطلاعاتی، اگرچه با خطرهایی از قبیل نداشتن حساسیت شرکای اطلاعاتی خارجی در خصوص حفاظت از اسرار مبادله‌شده و منابع مواجه است و امکان تبادل آن با کشورهای ثالث وجود دارد؛ اما همکاری با سازمان‌های ضداطلاعاتی خارجی کمک‌های فراوانی در زمینهٔ فعالیت‌های تهدیدگران فراهم می‌کند. آموزش‌های

ضداطلاعاتی یکی از حوزه‌های مهم همکاری اطلاعاتی و ضداطلاعاتی می‌تواند باشد. این آموزش می‌تواند در حوزه‌هایی مانند امنیت بهتر فناوری اطلاعات، شیوه‌ها و فنون اطلاعاتی عاملان تهدیدهای ترکیبی، شیوه‌های بازرسی و چگونگی حفاظت از مواد و مطالب حساس باشد.

۳) حوزه کارکردی حفاظت اطلاعات: حوزه‌های کارکردی حفاظت اطلاعات در یک کشور عبارت‌اند از:

- حوزهٔ توسعهٔ منافع و سیاست‌های امنیت ملّی کشور برای امن‌کردن امکان استقرار منابع، امکانات و ظرفیت‌های تحرک نهادهای ملی؛
- پایش و رصد تحولات در حوزه‌های ساختاری، عملیات، منابع انسانی، تجهیزات، فناوری و ده‌ها حوزهٔ مؤثر دیگر در امور اطلاعاتی و امنیتی در محیط منطقه‌ای و بین‌المللی که می‌تواند مزیت‌های حضور و برتری اطلاعاتی و امنیتی را دچار نوسان یا اختلال کند؛
- مدیریت‌پذیرسازی روندهای پیش روی که می‌تواند موجب بروز تحولات عمیق و جهش‌گونه شده و بسیاری از کارکردهای حفاظتی و اطلاعاتی را مواجه با آثار برتری‌ساز و یا ضربات شکننده کند، از جمله الزام‌های آینده‌نگاری حفاظتی آن است که می‌تواند در بستر فناوری‌ها، علوم حفاظتی، فنون عملیاتی، مدل‌های پنهان‌کاری، شیوه‌های مدیریتی و عمل شبکه‌ای در سامانه‌های ارتباطی نهادهای حفاظت اطلاعاتی پیاده‌سازی شود؛
- پیش‌بینی و طراحی سناریوهای رفتاری و عملکردی نهادهای ملّی در توسعه و فعالیت‌های بازیگری در نظام بین‌الملل و مخالفان منافع امنیت ملّی کشور که می‌تواند بسته و مجموعه‌ای از فعالیت‌های پنهان و نفوذی مخرب علیه منافع کشور و بروز نابسامانی و بحران در هماهنگی‌های توسعهٔ ملی را که بسترساز حضور دشمن در زوایای تاریک و دور از کنترل عمومی و جمعی باشد؛

• ترسیم تحولات در حفاظت اطلاعات می‌تواند گونه‌های سرعت، کنترل، جهت و گزینه‌های حرکت را نزد مدیران ملّی و سازمانی مجسم سازد، گرچه تخیّل در حفاظت اطلاعات اگر نتواند موجب گزینش اصلی در این چهار مدار باشد می‌تواند عنصر مخربی باشد. حفاظت اطلاعات هنر و فن هوشمندی است، زیرا همواره در مقابل ابتکار حریف قرار داد؛ بنابراین باید همواره موفقیّت‌ها را ترسیم و شبیه‌سازی کند تا بتواند نقاط جهش و سمت و سوی نفوذ و ضد نفوذ را رسم کند؛

• در حفاظت اطلاعات روحیهٔ تهاجمی به فرصت‌ها و کانون‌های تحول اصل است. امروز اگر نتوانیم به تجهیز و به‌روزآمدگی سازمان‌ها توجه کنیم در میان گرداب‌های فناوری و فرهنگ نرم تهدید به رده‌های انفعال و وابستگی سقوط خواهیم کرد، به‌روزشدگی فرهنگ حفاظت اطلاعات متناسب با آرمان‌ها و ارزش‌های اسلام ناب محمدی(صلی‌الله) می‌تواند تضمین واکنش فعال در برابر تهدیدهای نوین اطلاعاتی باشد. قدرت نرم، امنیّت نرم، فناوری نرم و فرهنگ مولد امروز از اساسی‌ترین الزام‌های حضور در کهکشان آینده است.

محورهای پارادایم جدید حفاظت اطلاعات: اگر بخواهیم حفاظت اطلاعات مؤثری باشیم ناگزیریم تا در قالب یک جامعهٔ اطلاعاتی و هماهنگ تعریف شده و هریک در جای خود قرار گیریم. این جامعه می‌تواند در بخش‌هایی هم عموم جامعه و نیز در برخی از کارکردها، نخبگان و تمامی نهادهای اجتماعی و فرهنگی را دربر بگیرد. در بخش‌های تصمیم‌سازی و تصمیم‌گیری به سمت ساختارهای حرفه‌ای و تخصصی به پیش رود؛ بنابراین ضرورت حکم می‌کند که حفاظت اطلاعات را بر بستر یک تغییر پارادایمی قرار داده و با مشارکت همه‌جانبه ملّی در ابعاد گوناگون، تابع موفقیت آن را در آینده ترسیم و اجزای معادله آن را تشریح و توصیف کنیم.

در واقع معتقدیم پارادایم حفاظت اطلاعات نوین در کشور خود نیاز به بررسی‌های عمیقی داشته تا در قالب ارزیابی‌های متنوعی امکان پیاده‌سازی و استقرار به خود بگیرد.

امروز جامعهٔ اطلاعاتی کشور در هجوم فراوانی شایعات، فرهنگ‌های کاذب شبکه‌ای، شبکه‌های جمع‌آوری اطلاعاتی، اینترنتی، ماهواره‌ای و ده‌ها کارکرد دیگر جاسوسی و براندازی است که خود را در پوشش ابزار و کارکردهای به‌ظاهر دموکراتیک ولی در واقع هژمونی و استکبار اطلاعاتی قرار داده‌اند که فریب‌خوردگان آن غافل از عضویت خائنانه خود در این شبکه هستند که کارکردهای وبلاگی و شبکه‌های اجتماعی و مستهجن و هرزه‌نگار که هریک بخشی از این مسئولیت را به‌عهده دارند نمونهٔ بارزی از این امر هستند.

بنابراین توسعهٔ فرهنگ حفاظت اطلاعاتی با توسعهٔ روشن‌بینی و هوشیارسازی ارکان مختلف جامعه باید قرین گردد تا بتواند بالاترین سطح مشارکت را در حمایت و حفاظت از منافع و هدف‌های امنیت ملّی به همراه داشته باشد و در شرایط بحرانی شاهد شکل‌گیری انسجام تمامی لایه‌ها در حمایت از این کارکرد باشیم.

امروز اگر در شبکه‌ها و سایت‌های اینترنتی شاهد عضوگیری سازمان‌های برانداز و سازمان‌های جاسوسی هستیم که قابلیت ارتباط امن و حفاظت شده را نوید داده و یا برای واگذاری اطلاعات از طریق قابلیت‌های اینترنتی میلیون‌ها دلار پیشنهاد می‌کنند لزوم هشدارهای حفاظتی و لایه‌های توجه و تدبر ملّی را گوشزد می‌کند.

نهادهای حفاظتی در کشور باید سرمشق و الگویی کارآمد را برای توقف این امور در پیش گیرند و در قلمرو تجویز سازمان‌های حفاظت اطلاعاتی باید تلاش شود محتمل‌ترین روندهای کنترل این وضعیت و تأمین امنیت اطلاعاتی کشور شناسایی و به عنوان راه‌کار تحقق مطلوب به‌گونه‌ای مناسب به جامعه ارائه گردد.

پارادایم جدید باید قادر باشد تمامی تصمیم‌ها را قابل انطباق و انعطاف با سطح تحولات و تهدیدهای نوین و هوشمند امروز و فردا کند به‌گونه‌ای‌که به‌صورت مستمر با شرایط تغییریافتهٔ محیطی بتواند، اصالت و کارآمدی خود را در حفاظت از زیرساخت‌ها و منافع ملّی حفظ کرده و رویکرد خلّاق و مهاجم خود را به آینده از این تخریب مصون گرداند. پارادایم جدید باید قادر باشد با اصلاح و تغییر قواعد ناکارآمد،

اقدام‌ها و برنامه‌های حفاظتی را در بهترین شرایط واکنش در برابر تهدیدهای محیطی و ضرورت‌های ملّی قرار دهد و بتواند علائم هشدار را که نشانگر بروز تهدیدها و تغییرهای متعارض جدید است به موقع شناسایی کند.

پارادایم جدید باید دربر گیرندهٔ شیوه‌های نوین پیش‌بینی، دیده‌بانی و ردزنی و شبیه‌سازی تهدیدهای حفاظتی و امنیتی باشد و فصل مشترک و شالودهٔ این شیوه‌ها، موجب پیش‌بینی و ترسیم آینده‌ای امن باشد. توانایی نظارت مستمر بر رخدادها و روندهای همراه و یا متعارض با منافع ملّی باید همواره از سوی مرکزی مقتدر و سامانه‌ای قابل اعتماد و وفادار به امنیّت ملّی صورت پذیرد و همواره با اتکاء به شواهد و قرائن مطمئن از تأمین امنیّت، شاخص‌های آن را در برنامه‌ریزی‌های حفاظت‌پایه و آینده‌محور مورد رصد و تقویت قرار دهد.

پارادایم جدید باید قادر باشد فرمول‌ها و معادلات حاکم بر ظهور تهدیدهای امنیتی در داخل و پیرامون مرزهای ملّی کشور را که در قالب‌های گوناگون و نوین پا به عرصه می‌گذارند شناسایی و شبیه‌سازی کرده و قابلیت‌های انهدام و یا کنترل آن را مدیریت کند و بر پایهٔ آن تصویری از آینده مخاطرات و ریسک‌های امنیتی را در سطح ملّی و سازمانی ارائه داده و ضرورت‌های حفاظت اطلاعاتی را گوشزد کند؛ بنابراین باید موضوع‌های حفاظت اطلاعات ملّی را با دقت و به‌گونه‌ای دنبال کرد که بتوان در سایهٔ آن معادلات ناامن‌ساز و بی‌آینده را در سیستم و سامانهٔ ملّی کنترل و یا به حریف برگرداند.

پارادایم جدید باید قادر باشد به توسعه و نفوذ فناوری در موضوع امنیّت ملّی با دقت و کنجکاوی نگریسته و ادامهٔ حضور آن را منطقی، تحت کنترل و بومی سازد باید توجه داشت که نیروهای پیشران فناوری در کشور و نظام بین‌الملل سعی می‌کنند خود را به‌ظاهر غیرقابل تغییر جلوه دهند و شیوه‌های پیش‌بینی‌پذیری مسیرهای آیندهٔ آن را به‌خدمت گیرند و آن را با بررسی و تحلیل علّی و متمایزسازی آن از روندهای توسعهٔ محدود و مانع از تهاجم اطلاعاتی و امنیتی آن شوند. این کارکرد در سازمان‌های حفاظت اطلاعاتی بسیار ظریف، دقیق، حساس و باید رو به رشد و تصاعد باشد که در غیر این صورت دقت‌ها را کاهش داده و به انحراف می‌کشد. پارادایم جدید باید بتواند مزیّت‌های

چشم‌گیر علمی و دانش‌بنیان را به‌خدمت گرفته و مسیرها و جهت‌های دقیق بروز تهدید و آسیب را با رویکردهای بومی و درونی و متکی بر فرهنگ‌سازی و تعمیق هویتی، مسدود کند تا بتواند پیشران‌های حفاظتی ملّت را از لایهٔ نخبگان و خبرگان و کارکنان انقلابی و دلسوز به مصاف مهارتی و حرفه‌ای با دشمنان متوجه سازد باید دانست که انقلابی جهانی در مطالبات عمومی صورت گرفته و پارادایم جدید باید قادر باشد تمامی تغییرهای محیطی را در حوزه‌های اجتماعی، اقتصادی، سیاسی، فردی، گروهی، فرهنگی، زیست‌محیطی در حوزهٔ رصد امنیتی و حفاظتی خود قرار داده و از ظرفیت‌های دگرگون‌ساز و تحول‌آفرین در جابه‌جایی قدرت و افزایش تنش و تعارض غافل نگردد.

در پایان باید تأکید کنیم اگر پارادایم جدید حفاظت اطلاعاتی به بهبود، کنترل و هوشمندسازی کارکردهای امنیتی و ترسیم چند منظوره، نرم و سازگاری با محیط قدرت توجه کند می‌تواند کارکردهای خود را در شبکه‌ای امنیت‌ساز و آینده‌گرا نشانه رود و شیب منحنی علوم و فناوری را به سمت منحنی متمایل به عموم در امنیت ملّی کند که در این صورت نشان از کوتاه‌تر شدن هرچه بیشتر چرخهٔ زمانی ناامن‌تر است. در آن برهه است که می‌توان از تغییرهای شتابنده و غیرقابل پیش‌بینی بودن برخی از روندهای آینده بیمی به‌خود راه نداده و ثبات و پویایی امنیتی کشور و سازمان‌ها را تضمین کرد.

روش‌شناسی تحقیق

این تحقیق از انواع تحقیقات کیفی است که با بهره‌گیری از روش موردی- زمینه‌ای انجام شده و اطلاعات لازم به شیوهٔ کتابخانه‌ای و میدانی (مصاحبه با خبرگان) تهیه و داده‌های جمع‌آوری شده با روش داده‌بنیاد، تحلیل و دسته‌بندی گردیده است. جامعهٔ آماری در این تحقیق شامل نخبگان امنیتی و اطلاعاتی همچون مدیران، رؤسا و فرماندهان سازمان‌های امنیتی و حفاظت اطلاعاتی و حراستی بوده که دارای تحصیلات تکمیلی یا مدیریتی در دستگاه‌های اطلاعاتی و امنیتی کشور هستند.

حجم نمونه در روش کیفی بنابر سؤال پژوهش، منابع مادی، زمان و همچنین تعداد پژوهشگر درگیر و... تعیین می‌گردد و فزونی حجم نمونه ضرورتاً روایی آن را بالا

نمی‌برد و حتی گاهی می‌تواند از دقت و غنای نمونه معرف جامعه نیز بکاهد. حجم نمونهٔ این تحقیق با استفاده از دو مدل گلوله برفی و نیز نمونه‌گیری هدفمند از میان استادان، مدیران و فرماندهان با تجربهٔ سازمان‌هایی که در حوزهٔ امور حفاظت اطلاعاتی و امنیتی که دارای ویژگی‌های زیر هستند انتخاب می‌شوند؛ و نمونه‌گیری تا زمان تحصیل اشباع نظری ادامه می‌یابد:

- حداقل دارای ده سال سابقهٔ مدیریت در سازمان‌های امنیتی و حفاظت اطلاعاتی و حراستی؛
- استادان حوزهٔ امنیتی و اطلاعاتی با تجارب عملی خدمت در سازمان‌های اطلاعاتی و حفاظت اطلاعاتی؛
- رؤسا و مدیران سازمان‌های جامعهٔ اطلاعاتی دههٔ اخیر.

در تحقیق کیفی از یک یا چند شیوه برای گردآوری اطلاعات و داده‌ها استفاده می‌گردد در این تحقیق روش گردآوری اطلاعات ترکیبی از روش‌های مصاحبه و مشاهدات میدانی و اسنادی بوده است.

روش تحلیل داده‌ها

داده‌های این تحقیق با استفاده از مدل‌ها و شیوه‌های تحلیلی نظریهٔ مبنایی یا داده‌بنیاد صورت می‌گیرد در این روش، جمع‌آوری و تحلیل داده‌ها به‌طور آگاهانه و هم‌زمان صورت می‌گیرد. در تئوری داده‌بنیاد برای جمع‌آوری، تحلیل و نظریه‌پردازی بر اساس داده‌ها، رویه‌های نظام‌مند صورت می‌پذیرد. تحلیل داده‌ها در روش کیفی و روش داده‌بنیاد مستلزم انجام سه فعالیت تلخیص داده‌ها، عرضهٔ داده‌ها و نتیجه‌گیری است که به‌صورت کدگذاری و تحلیل مفاهیم، مقوله‌ها و گزاره‌ها یا فرضیه‌ها صورت می‌گیرد. در این پژوهش داده‌ها از روش داده‌بنیاد[1] مورد تحلیل قرار گرفته است؛ بنابراین به‌منظور ارائه الگوی حفاظت اطلاعات، بر اساس یافته‌ها ۱۳۹ مفهوم با در نظر گرفتن ماهیت نمونه‌برداری (جهت‌گیری کلی)، از متون مصاحبه‌ها استخراج و کدبندی و پس از ترکیب مفاهیم، ۱۷ مقوله به‌دست آمد.

1. Grounded Theory

نتیجه‌گیری

برای رسیدن به الگوی نهایی با استفاده از روش داده‌بنیاد و مبتنی بر ظهور مفهومی داده‌ها و دیدگاه محقق مفاهیم و مقوله‌ها تحصیل گردید و در ادامه عناصر اصلی الگو استخراج شد. در این الگو سه مؤلفه اصلی تهدیدهای ترکیبی، منافع ملی و هدف‌های ملی تبیین کننده ضرورت و اهمیت ایجاد چنین سیستم و نهادی در کشور و تعیین‌کنندهٔ چارچوب کلی آن است، همچنین شناخت و درک از تهدیدهای ترکیبی جدید و پیش‌رو و آسیب‌هایی که باعث درز و سرقت اطلاعات ملی در کشور می‌گردد این ضرورت را نمایان می‌کند که می‌باید متناسب با شکل جدید تهدیدها، الگوی جدیدی نیز برای مقابله با آن پیش‌بینی گردد. در الگوی حفاظت اطلاعات فقط سطح راهبردی مورد نظر بوده و حفاظت اطلاعات به‌طور مستقیم درگیر سطوح پایین‌تر اطلاعات نمی‌گردد. این الگو دارای سه بعد اصلی به این شرح است:

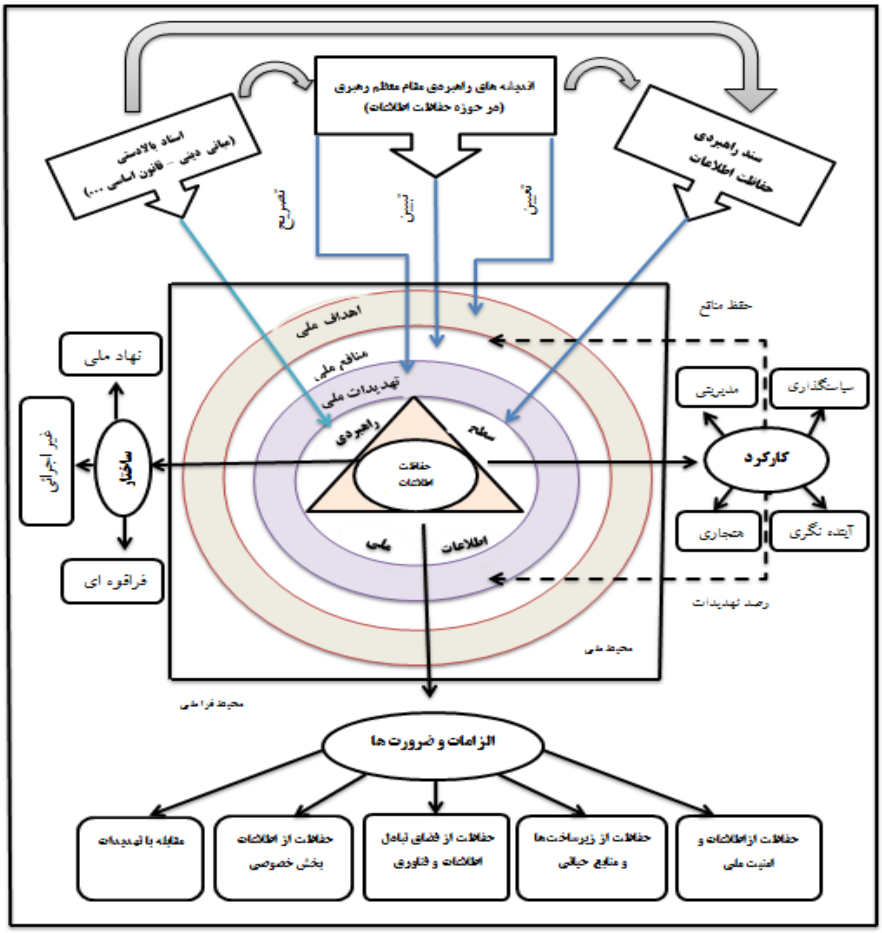
۱) بُعد کارکردی که شامل کارکردهای مدیریتی، سیاست‌گذاری، آینده‌نگری و هنجاری است؛

۲) بُعد ساختاری حفاظت اطلاعات که مبین این موضوع است که حفاظت اطلاعات می‌باید ساختاری ملی و دارای جایگاه فراقوه‌ای بوده و ماهیتی غیراجرایی (سیاست‌گذار و نظارت‌کننده و...) داشته باشد؛

۳) بُعد الزام‌ها و ضرورت‌های حفاظت اطلاعات که در پنج حوزهٔ الزام‌های مربوط به مباحث امنیتی- اطلاعاتی، حفاظت از زیرساخت‌ها و منابع حیاتی، حفاظت از فضای تبادل اطلاعات و امنیت فناوری، حفاظت از اطلاعات بخش خصوصی و الزام‌های مربوط به تهدیدهای ترکیبی قابل تقسیم‌بندی و ارائه است.

بدیهی است این تحقیق به‌دنبال ارائه یک ساختار جامع یا تبیین وظایف و اختیارات برای حفاظت اطلاعات نبوده بلکه با توجه به بدیع‌بودن موضوع، درصدد است تا با بهره‌گیری از نظرهای نخبگان به روش علمی و با استفاده از ظرفیت‌های روش تحقیق داده‌بنیاد، نسبت به تئوریزه کردن مبانی و الزام‌های این نهاد اقدام کرده و الگویی ارائه کند تا مبتنی بر مفاهیم استخراج شده، عمده مؤلفه‌های اثرگذار در این الگو احصاء و

تبیین گردد. از این رو در الگوی ارائه شده در بُعد ساختاری، فقط به چارچوب‌های کلی آن اشاره شده است و بُعد کارکردی نیز به نحوی دسته‌بندی شده تا به‌عنوان مبنایی، برای تعیین وظایف و اختیارات این نهاد مورد استفاده قرار گیرد. با توجه به چالش‌های موجود در ایجاد هماهنگی و تعامل در نظام امنیتی، ارائه این الگو می‌تواند راهبردی عملی برای پاسخ به ضرورت‌های امنیتی حال و آینده باشد و همچنین بستری برای مطالعات آینده فراهم کند. بر اساس یافته‌ها و نتایج این تحقیق، الگوی راهبردی حفاظت اطلاعات در برابر تهدیدهای ترکیبی برابر شکل زیر است:



الگوی راهبردی حفاظت اطلاعات

پیشنهادها

پیشنهادهای کاربردی حاصل از تحقیق حاضر به شرح ذیل است:

۱) با تشکیل کمیسیون‌های ویژه، مبانی حقوقی و قانونی مقابله با تهدیدهای ترکیبی تبیین و ابلاغ گردد؛

۲) خلأهای موجود در ساختار اطلاعاتی- امنیتی کشور در برابر تهدیدهای ترکیبی احصا و حوزه‌های حفاظتی متناسب از زیرساخت‌ها گرفته تا ارزش‌های قابل حفاظت، به عنوان یک ضرورت بررسی و چاره‌اندیشی شود؛

۳) سند راهبردی حفاظت اطلاعات در برابر تهدیدهای ترکیبی در سطح جامعه اطلاعاتی به‌روزرسانی، تدوین و اجرایی شود؛

٤) آموزش‌های عمومی، تخصصی، توجیه و آگاه‌سازی در سطح ملی در حوزهٔ حفاظت از اطلاعات در قبال تهدیدهای ترکیبی در اولویت قرار گیرد تا فهم مشترک و یکسان در این حوزه ایجاد گردد.

منابع

افضل، رضا (۱۳۹۵)، *اصول و مبانی حفاظت*، تهران: چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی.

آستانا،اِن‌سی،نیرمال،آنجالی (۱۳۸۸)، *مدیریت اطلاعات و امنیت*، ترجمهٔ معاونت پژوهشی، تهران: دانشکده اطلاعات.

برکوویتر، بوریس‌دی و گودمن،آلن‌ای (۱۳۸٤)، «بهترین حقایق اطلاعات در عصر اطلاع رسانی»، تهران: نشر دانشکدهٔ امام محمدباقر(علیه‌السلام).

ترورتون، گری‌گوری.اف (۲۰۰۱)، *تجدید ساختار اطلاعات در عصر اطلاع‌رسانی*، تهران: نشر دانشکدهٔ امام محمدباقر(علیه‌السلام).

حسن‌بیگی، ابراهیم (۱۳۹۰)، مدیریت حفاظت اطلاعات ملی و آینده‌نگاری، تهران: همایش حفاظت اطلاعات ملی، سپاه پاسداران انقلاب اسلامی، دانشکدهٔ امام(علیه‌السلام).

حسن‌بیگی، ابراهیم (۱۳۹۰)، *مدیریت راهبردی*، تهران: سمت.

حضرت امام خمینی رحمت‌الله علیه (۱۳۸۲)، *صحیفه نور*، ج ۱۱، ۱۵، ۱۹، تهران: دفتر حفظ و نشر آثار امام خمینی رحمت‌الله علیه.

حضرت آیت‌الله العظمی امام خامنه‌ای(مدظله‌العالی) (۱۳۹۰)، *اوامر و منهیات حفاها*، دفتر فرماندهی معظم کل قوا.

حضرت آیت‌الله العظمی امام خامنه‌ای(مدظله‌العالی) (۱۳۹٤)، *نرم‌افزار حدیث ولایت*، مجموعه رهنمودهای مقام معظم رهبری حضرت آیت‌الله العظمی امام خامنه‌ای(مدظله‌العالی)، مرکز تحقیقات کامپیوتری علوم اسلامی.

حمیدزاده، محمدرضا (۱۳۷۹)، *پویایی برای سیستم‌ها*، تهران: نشر دانشگاه شهید بهشتی.

شولسکی، آبرام (۱۳۸۱)، *نبرد بی‌صدا: درک دنیای اطلاعات*، ترجمهٔ معاونت پژوهشی دانشکدهٔ امام باقر(ع)، تهران: نشر دانشکدهٔ امام محمدباقر(علیه‌السلام).

عاصم، ابراهیم و اشرف العیسوی (۱۳۸۸)، *سرویس‌های اطلاعاتی و نقش آنها در هزاره سوم*، ترجمهٔ عسکر جلالیان، تهران، دانشکده اطلاعات.

عصاریان‌نژاد، حسین (۱۳۷٦)، *سازمان‌های اطلاعاتی و حفاظت اطلاعاتی*، تهران: دانشکده فارابی.

کتولی‌نژاد، خدابخش (۱۳۹۰)، «حفاظت اطلاعات آینده و مدیریت دانش»، *فصلنامه تخصصی ساحفاناجا*، تهران: حدیث کوثر.

گادسون روی و دیگران (۱۳۸۳)، «اطلاعات آمریکا بر سر دو راهی»، ترجمهٔ معاونت پژوهشی دانشکده، مجید نوری، معاونت پژوهشی دانشکده امام محمدباقر(علیه‌السلام).

مشیدیان، هادی و حسین اکبری (۱۳۹۵)، «بی‌نام»، *فصلنامه اطلاعاتی و حفاظتی جامعه اطلاعاتی*، سال هفتم، شماره دوم.

میرجعفری، سیداصغر (۱۳۹۳)، «ارائه الگوی راهبردی ساحفاودجا»، *رساله دکترا دانشگاه دفاع ملی*.

Barnea, A. (2017). "Counterintelligence: Stepson of the intelligence discipline", Israel Affairs, vol.23,no.4.

Bauer, Alain, (2016). "Who Is The Enemy? Terrorism As An Unidentified Fighting Object", avaliable at International Institute for Counter-Terrorism. Retrieved from https://www.ict.org.il/Article/ 1774/who-is-the-enemy-terrorism-as-an-unidentifiedfighting-object#gsc.tab=0

Britovšek, Jaroš, (2018)."Comparing Counterintelligence and Counterterrorism – Similarities, Issues and Solutions", Journal of Criminal Justice and Security, Vol. 20,No. 2.

Cogan, Charles, (2004), "Hunters not Gatherers: Intelligence in the

Duvenage and Basie Vs, (2015). «Cyber counterintelligence: Back to the future»,Journal of Information Warfare,Vol.13, Issue 4

Gentry John A. (2015): "Toward a Theory of Non-State Actors' Intelligence",Intelligence and National Security, DOI: 10. 1080/02684 527.2015.1062320.

McGeehan, Timothy, P. (2018).Countering Russian Disinformation Parameters Quarterly, Vol. 48 No. 1.

Mobley Blake W. (2012).Terrorism and counterintelligence: how terrorist groups elude detection, New York: Columbia University Press.

Monaghan, Sean, (2019).Countering Hybrid Warfare So What for the Future Joint Force? PRISM, V.8, No. 2. Nye Joseph S. (1994).

"Peering into the Future «Foreign Affairs, Vol. 73, No. 4
Rietjens, Sebastiaan (2020)."A warning system for hybrid threats – is it possible? Hybrid CoE StratgicAnalysis, No.22
Moravej Kaveh and Díaz, Gustavo, (2007)."Critical Issues in Contemporary counterintelligence", UNISCI Discussion Papers, No, 13
Prunckun Hank, (2019). Counterintelligence: Theory and Practice, London: Rowman & Littleld.
Redmond Paul J. (2010). The Challenge of Counterintelligence in Loch Johnson, The Oxford Handbook of National Security Intelligence, New York: Oxford University Press,
Strohm,Chris (2020). "U.S. Spy Agencies Move to Counter Foreign Influence Operations", available athttps://www.Bloomberg.com/ news /articles/2020-02-1/u-s-spy-agencies-move-to-counter-foreign-influence -operations.
twenty-first century, in (eds) L.V. Scott and P.D. Jackson Understanding Intelligence in the Twenty-First Century, New York, Rutledge.
Van Cleave, Michelle K (2013). "What is Counterintelligence? A Guide to Thinking and Teaching about CI", Journal of U.S. Intelligence Studies Vol.20.No.2.