فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)
سال بیستم: شماره ۷۷- بهار ۱۴۰۱
صص: ۱۰۳ - ۱۵۴
تاریخ دریافت: ۱۴۰۰/۹/۶
تاریخ پذیرش: ۱۴۰۰/۱۱/۲۰

Amniat Pajouhi: Security Research Quarterly
Vol.20, No.77,Spring 2022
P-P: 103 - 154

اشراف اطلاعاتی سایبرمحور (تبیین مؤلفه‌ها، پیامدها و الزامات)

رضا حسینی[۱]
جمشید نصرت آبادی[۲]

چکیده:

امروزه پیشرفت ارتباطات سایبری باعث شده است که سازمان‌های امنیتی در کسب اشراف اطلاعاتی و نیل به مأموریت‌های محوّله با چالش روبه‌رو گردند. در این پژوهش کاربردی با استفاده از روش توصیفی – تحلیلی و با تکنیک مصاحبه و پرسش‌نامه محقق‌ساخته که روایی و پایایی آن تایید گردیده است مؤلفه‌ها، پیامدها و الزامات اشراف اطلاعاتی سایبرمحور تبیین می‌گردند. با انتخاب حجم نمونه صد نفری از خبرگان و کارشناسان در زمینه سایبری، داده‌های توصیفی با کمک نرم‌افزار SPSS مورد تحلیل قرار گرفته و یافته‌های تحقیق حاکی از آن است که ۹۳ درصد در حدّ زیاد و خیلی زیاد موافق سازوکارهای مرتبط با درک سایبری، ۹۶ درصد در حدّ زیاد و خیلی زیاد موافق سازوکارهای مرتبط با فهم سایبری و ۷۷ درصد در حدّ زیاد و خیلی زیاد نسبت به تجسّم سایبری به عنوان مولفه‌های اشراف اطلاعاتی سایبرمحور نظر مساعد داشته و بهره‌گیری از الزامات دانش، مهارت، زیرساخت‌ها، نیروی‌انسانی متخصص، نظامات سایبری و دستورالعمل‌ها را موجبات فراهم آمدن پیامدهایی از قبیل برتری عملیاتی، پیشگیری از غافلگیری، خنثی‌سازی و ارتقاء امنیت سایبری می‌دانند.

واژگان کلیدی: اشراف اطلاعاتی، فضای سایبر، امنیت سایبری، اشراف اطلاعاتیِ سایبرمحور

۱. کارشناس ارشد مدیریت اطلاعات دانشکده علوم و فنون فارابی، نویسنده مسئول
Reza.Hoseini523@gmail.com
۲. استادیار مدیریت راهبردی فضای سایبر دانشکده علوم و فنون فارابی
Dr.Nosratabadi110@gmail.com

جستارگشایی

یکی از موضوعات مهم و اساسی در عصر کنونی که آن را عصر دیجیتال می‌نامند، سرعت، پیچیدگی و نفوذ فضای سایبر و فناوری اطلاعات و ارتباطات است و این موضوع تمامی ابعاد زندگی بشر را تحت تأثیر قرار داده و به واسطه تغییرات، موجودیت و عرصه کنشگری تمامی نهادها و سازمان‌ها به درک صحیح و به‌موقع از این دگرگونی‌ها و برنامه‌ریزی برای مواجه شدن با آن گره خورده است. با توجه به شرایط و محیط فضای سایبر، شناخت و اشرافیت بر نقاط بحرانی، عوامل اثرگذار خارجی و داخلی و همچنین رصد علائم بروز تهدیدات در این فضا با هدف پیشگیری از غافلگیری راهبردی ضرورت دارد.

در سال ۲۰۱۰، ایالات متحده به طور رسمی فضای سایبری را به عنوان حوزه پنجم قدرت به رسمیت شناخت و با ایجاد واحد فرماندهی سایبری ایالات متحده، فرماندهی یکپارچه آن از نیروهای مسلح به فرماندهی راهبردی ایالات متحده واگذار شد. فرمان سایبری ایالات متحده مرتبط با حوزه‌های زمین، دریا، هوا و فضا می‌باشد. اگرچه فضای سایبری یک قلمرو مجازی است، اما نفوذ جهانی را می‌توان سریع‌تر و فراگیرتر از هر قلمرو دیگری در آن مورد بررسی قرار داد. فضای سایبری برای اهداف دیپلماتیک و اطلاعاتی بسیار مؤثر است. فناوری‌های اینترنتی موجب اشتیاق عموم مردم به اخبار فوری شده و دولت‌ها را برای انجام دیپلماسی دیجیتالی تحت تاثیر قرار می‌دهد. دولت‌ها از فضای اینترنتی برای اطلاع‌رسانی به شهروندان در مورد سیاست‌های عمومی، بیان موقعیت‌های دیپلماتیک به صورت پویا و حتی گسترش اطلاعات غلط استفاده می‌کنند. بازیگران غیردولتی نیز فضای سایبری را برای دیپلماسی و ابتکارات اطلاعاتی استفاده می‌کنند. القاعده برای جذب اعضای جدید از اینترنت استفاده کرده و با استفاده از آن برای ساخت دستگاه‌های تروریستی و بمب‌گذاران انتحاری ایجاد انگیزه می‌کند. در بیداری اسلامی، انقلابیون به طور مؤثر از رسانه‌های اجتماعی برای تبلیغ برنامه‌های سیاسی، افزایش آگاهی و جذب حمایت و بودجه استفاده کرده و حتی فعالیت‌های ده‌ها هزار معترض را در زمان واقعی هماهنگ کردند. ظهور فضای مجازی و مفهوم قدرت سایبری نیاز به ارزیابی چگونگی تحقق قدرت و نفوذ در یک جهان به هم پیوسته دارد. از آنجاکه فضای مجازی فاقد مرزهای فیزیکی است، ملت‌ها قدرتی برای حفظ مرزها و یا راه‌هایی برای تهدید مرزهای همسایه با استفاده از تعاریف متداول قدرت را ندارند (نجفی و حسینی، ۱۴۰۰:۶) لذا این مهم لزوم و اهمیت داشتن اشراف اطلاعاتی بر این فضا را دوچندان می‌کند. اطلاعات سایبری پایهٔ طراحی و هدایت عملیات و حفظ برتری در تمام ابعاد است که به سازمان‌های اطلاعاتی و امنیتی امکان می‌دهد که کنترل تهدیدات و اشراف بر محیط اطلاعاتی و عملیاتی را احراز نماید. تأمین اطلاعات سایبری به‌موقع و دقیق به درک سازمان‌های اطلاعاتی و امنیتی از دشمن و محیط عملیاتی کمک می‌نماید. هیچ عملیاتی را نمی‌توان با امید واقعی به موفقیت طراحی نمود مگر آن‌که اخبار سایبری کافی راجع به حریف

و محیط کسب کرده و آن را به اطلاعات سایبری تبدیل کرد. داشتن اطلاعات سایبری پنهان از نیروهای حریف و هدف، اگر چه کاری صعب و پُرهزینه است اما منبعی مهم برای اعمال قدرت است. انفعال در چرخه اشراف اطلاعاتی، کاهش اقتدار سایبری، غفلت از اهمیت اطلاعات سایبری به عنوان دارایی نامشهود سازمان‌های اطلاعاتی و امنیتی از جمله آثار زیان‌بار عدم توجه مناسب به اشراف اطلاعاتی در حوزه سایبر می‌باشد (بیابانی و اسفندیاری، ۱۳۹۶: ۴۲).

قدرت سایبری امروزه بُعد مهمی از زیست‌وارهٔ جهانی را شکل می‌دهد. اطلاعات و فناوری‌های اطلاعاتی در سپهر سیاسی، اقتصادی، و نظامی نقشی حیاتی ایفا می‌کنند و مقدمات فعالیت‌های عملیاتی را فراهم می‌آورند. با گسترش روزافزون فضای سایبری، نگرانی‌های زیادی هم در این باره ایجاد می‌شود؛ این گسترش درکنار آثار مثبت در بهبود زیست جهانی، برخی ابعاد منفی نیز دارد که حتی ممکن است آثار آن مخرب‌تر از جنگ‌های نظامی باشد و امنیت ملی و حیات مردم را به چالش بکشاند (زابلی‌زاده، ۱۳۹۷: ۴۸). مقام معظم رهبری (مد ظله العالی) در دیدار اعضای هیئت دولت در تاریخ ۰۳/۰۶/۱۳۹۵ در خصوص اهمیت فضای سایبر می فرمایند:"...فضای مجازی واقعاً یک دنیای رو به رشد غیرقابل توقف است، یعنی واقعاً آخر ندارد؛ آدم هر چه نگاه می کند، آن چیز اول بلا آخر، فضای مجازی است. هر چه انسان پیش می‌رود در این فضا، این همین طور ادامه دارد. این فرصت‌هایی در اختیار هر کشوری می گذارد، تهدیدهایی هم در کنارش دارد، ما بایستی کاری کنیم که از آن فرصت‌ها حداکثر استفاده را بکنیم، از این تهدیدها تا آنجایی که ممکن است خودمان را بر کنار نگه داریم." بر این اساس اشرافیت بر فضای سایبر و شناخت تهدیدات و فرصت های آن و کسب برتری در آن باید در دستور کار سازمان‌های مختلف به ویژه سازمان‌های اطلاعاتی و امنیتی قرار گیرد. با توجه به ماهیت متغیر پدیده‌ها در عصر اطلاعات و پیچیدگی‌های فضای سایبر و شکل‌گیری تهدیدات نوین در این حوزه، اشراف اطلاعاتی سایبرمحور یکی از نیازهای اساسی و بنیادین سازمان‌های اطلاعاتی وامنیتی است. دغدغه اصلی محقق در این پژوهش که جنبه نوآورانه تحقیق نیز به شمار می رود، پرداختن متمرکز بر حوزه اشراف اطلاعاتی سایبر محور و تبیین مولفه‌ها، پیامدها و الزامات نیل به اشراف اطلاعاتی در فضای سایبر می‌باشد.

سازمان‌های اطلاعاتی و امنیتی به عنوان یکی از سازمان‌های متولی امر امنیت هم در حوزه تهاجم و هم در حوزه دفاعی ارتباط زیادی با این فضا دارند (محمودزاده و اسماعیلی،۱۳۹۷:۲۰۴). اشراف اطلاعاتی سایبرمحور یکی از نیازهای اساسی و بنیادین و در حقیقت یکی از عوامل موفقیت سازمان‌های امنیتی – اطلاعاتی است که می‌تواند نیازمندی های اطلاعاتی و عملیاتی این سازمان‌ها را در فضای پیچیده سایبر تأمین نماید. برتری اشراف اطلاعاتی سایبرمحور، همان مزیت در انجام عملیات است که این مزیت با توانایی در جمع‌آوری، پردازش و انتشار اطلاعات سایبری به طور پیوسته فراهم می‌شود. در همان حال با ایجاد عدم توانایی در حریف برای انجام دادن موارد فوق وی را از آن محروم می کند. برتری اشراف اطلاعاتی سایبرمحور

در یک محیط غیرعملیاتی یا در موقعیتی که در آن هیچ‌گونه مخالف یا مجرم معینی وجود ندارد، زمانی حاصل می‌شود که نیروهای خودی، اطلاعات سایبری لازم برای رسیدن به اهداف اطلاعاتی را در اختیار دارند. مسئله اصلی و سوال کلیدی در این پژوهش آن است که مؤلفه‌ها، پیامدها و الزامات اشراف اطلاعاتی سایبرمحور در سازمان‌های اطلاعاتی و امنیتی چیست؟ در این پژوهش که مبتنی بر روش توصیفی و تحلیلی و همراه با فرضیه اکتشافی است محقق سعی دارد به منظور پاسخ به مسئله کلیدی پژوهش، ضمن تبیین ابعاد و اصول مختلف اشراف اطلاعاتی سایبر محور، به شناخت مؤلفه‌ها، پیامدها و الزامات پیاده‌سازی آن در سازمان‌های اطلاعاتی و امنیتی بپردازد.

مبانی نظری و مفاهیم:

فضای سایبر[1]

از لحاظ لغوی در فرهنگ‌های مختلف، سایبر به معنی مجازی و غیرملموس و مترادف انگلیسی (*Virtual*) است. در زبان فارسی سایبر را مجازی و Space را فضا ترجمه کرده‌اند و ترکیب آن را فضای مجازی می‌گویند. معادل واژه سایبر در فارسی، فضای تولید و تبادل «فتا» عنوان می‌شود. واژه سایبر از لغت یونانی (*Cybernetic*) به معنی سکان‌دار یا راهنما مشتق شده است. واژه «فضای سایبر» را نخستین بار «ویلیام گیبسون[2]» نویسنده داستان علمی – تخیلی در کتاب «نورومنسر» در سال ۱۹۸۴ به‌کار برده است. فضای سایبر در معنا به مجموعه‌هایی از پیوندهای درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. برخلاف فضای واقعی، در فضای سایبر نیاز به جابه‌جایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات «ماوس» صورت می‌گیرد (موسوی و مستجابی سرهنگی،۱۳۹۲:۲۴).

امنیت سایبری[3]

در برداشت سنتی، امنیت منحصراً در نبود خطرات فیزیکی خلاصه می‌شد، در چنین شرایطی اختلال در امنیت به یک حمله فیزیکی بستگی داشت. اما امنیت در معنای نوین آن را نمی‌توان به تنهایی در چارچوب مرزها و در روابط دولت – ملت‌ها جستجو کرد. امنیت سایبر را می‌توان به استفاده از ابزارهای مرتبط با ایمن‌سازی، توانمندسازی و صحت اطلاعاتی دانست که پردازش، حفاظت و ارتباط‌شان به وسیله ابزارهای الکترونیکی امکان‌پذیر است (برقعی،۱۳۹۳:۸۶). در واقع امنیت در فضای سایبری، امنیت در قسمت زیرساخت و شریان‌های اطلاعاتی می‌باشد، ایجاد فرصت جدید برای شغل‌ها و ممالک در محیط خودکارسازی، تجارت الکترونیکی، تبادل و همکاری منجر به تولید هدفمند، ذخیره‌سازی و بهره‌برداری از اطلاعات حساس و حیاتی شده است. وابسته بودن به شبکه‌های پرسرعت و قدرتمندشدن پردازشگرها

1. *Cyberspace*
2. *William Gibson*
3. *Cybersecurity*

روزبه‌روز در حال افزایش است که باعث قرار گرفتن سیستم‌ها در معرض خطرات طبیعی و حتی بزهکاری و تروریسم سایبری شده، که نیازمند نظارت و مدیریت می‌باشد (پورقهرمانی،۱۳۹۹:۱۴۱).

اشراف اطلاعاتی

اشراف اطلاعاتی عبارت است از آگاهی به موقع و همه‌جانبه دستگاه اطلاعاتی از علائم، زمینه‌ها و بسترهای بالقوه و بالفعلِ رویدادها، تصمیمات و تحرکات حریفان و کاربرد مؤثر این آگاهی‌ها برای تأمین امنیت و حفظ و صیانت داشته‌ها از طریق ابزار و روش‌های جمع‌آوری به ویژه ابزار نیروی‌انسانی. اشراف اطلاعاتی هدف نیست بلکه ابزاری برای رسیدن به هدف که همان انجام مأموریت است، می‌باشد (مزینانی، ۱۳۹۲:۲۲۳).

اشراف اطلاعاتی محصول تفکر سیستمی بوده و هرگونه اقدامی مستلزم اشرافیت بر اهداف و موضوعات باشد، می‌تواند تهدیدها را خنثی و از صرف هزینه‌های اضافی جلوگیری نموده و به شکلی دقیق و عمیق واقعیت‌های عینی و ذهنی را در ابعاد مختلف به گونه‌ای روشن و شفاف به تصمیم‌سازان ارائه دهد (عصاریان،۱۳۹۱: ۷۸-۷۶).

در واقع اشراف اطلاعاتی فرآیندی است که سازمان‌های اطلاعاتی با گسترش و استمرار تلاش جمع‌آوری و تبادل اطلاعات بین‌سازمانی با استفاده از منابع رسمی، فنی، آشکار و پنهان و با ارزیابی، تجزیه، تحلیل و تفسیر همه معلومات بدست آمده برای گسترش داشته‌های اطلاعاتی و افزایش ظرفیت‌های دستیابی به آگاهی و شناخت تهدیدها، آسیب‌ها و فرصت‌ها به منظور برتری اطلاعاتی و تأمین نیازمندی‌های اطلاعاتی در حوزه‌های خودی و حریف در راستای کاهش نقاط کور و غیرقابل دسترس در جهت پیش‌گیری و خنثی‌سازی انجام می‌پذیرد (خواجه امیری، ۱۳۸۹:۳۵).

برتری اطلاعاتی نوعی از توانایی در جمع آوری، پردازش و انتشار اطلاعات برای مقابله با تحرکات حریف جهت انجام این کار است. در واقع برتری اطلاعاتی، درک جامع‌تر اطلاعات و روابط نسبت به حریف می‌باشد. با داشتن اطلاعات با کیفیت‌تر و اطلاعات سطح بالاتر، می‌توان در جایگاه بالاتری نسبت به دیگران قرار گرفت. کسانی که برتری اطلاعاتی داشته باشند، می‌توانند دیگران را که از برتری اطلاعاتی کم‌تری برخوردارند، به کنترل خود درآورند (*Helokunnas;Kuusisto,2003:3*).

با توجه به اهمیت موضوع، پژوهش‌های زیادی درباره واژگان کلیدی پژوهش انجام شده است که محور اصلی این آثار پرداختن به عوامل و ابزارهای دستیابی به اشراف اطلاعاتی بوده است. در زیر به تعدادی از عناوین که نسبت به سایر موارد شاخص‌تر بودند و بیشتر از سایر منابع، اشراف اطلاعاتی سایبرمحور را مورد واکاوی قرار داده‌اند به‌اختصار ارائه می‌گردد.

پورمنافی (۱۳۹۶) برای طراحی الگوی راهبردی اشراف اطلاعاتی ناجا برای تحقق اشراف اطلاعاتی سه

حوزهٔ محیطی، موضوعی و فردی اشراف اطلاعاتی را مدنظر قرار داده است. با توجه به نتایج این تحقیق، این الگو با توان آگاه‌سازی، پیشگیری و تولید فرصت، مجهز به سامانه‌های اطلاعاتی و هوشمند با تعاملات سازنده و فراگیر، با هدف کنترل و پایش اوضاع از هر لحاظ و اولویت دادن به آموزش و توانمندسازی، مشارکت مردمی، آینده‌نگاری و سناریوپردازی، توجه به سرمایهٔ انسانی، هم‌افزایی جامعهٔ اطلاعاتی درون ناجا، کنترل و ترمیم ناشی از شرایط جدید را رقم زده، از غافلگیری جلوگیری، با اقدام به هنگام، سرعت، افزایش قابلیت‌ها، شناسایی تهدیدات و آسیب‌پذیری‌ها برای برقراری نظم و امنیت حفظ و توسعهٔ آن به نحو مطلوب تقویت تأمین و استقرار امنیت پایدار مردمی و قابلیت مدیریت اطلاعاتی اثربخش برای تصمیم‌سازی و تصمیم‌گیری را به دنبال خواهد داشت.

مطالعه گروهی در دانشگاه عالی دفاع ملی (۱۳۹۳) شاخص‌های اشراف ملّی اطلاعات در ارتش جمهوری اسلامی ایران را مورد مطالعه قرار داده که نتایج حاکی از آن است که بقاء و رشد جمهوری اسلامی ایران مستلزم توانایی برای واکنش به موقع و مناسب در برابر تغییرهای پی‌درپی محیطی است. فقط کشورهایی می‌توانند ضرورت‌ها و تغییرهای محیطی را به موقع پیش‌بینی کنند و بقای خود را در محیط دائماً ادامه دهند که رفتارهای فعلی آنان مبتنی بر تجربه‌های گذشته، درک موقعیت فعلی و معطوف به هدف‌های آینده، از طریق شناخت شاخص‌های اشراف ملی اطلاعات که باعث تقویت هویت جمهوری اسلامی ایران در سطح بین‌المللی شده که منجر به افزایش سطح اعتماد تصمیم‌گیران لشکری و کشوری می‌گردد و از غافلگیری کشور در عرصه‌های مختلف جلوگیری می‌نماید لذا اشراف ملّی اطلاعات یکی از اساسی‌ترین وظایف برنامه‌ریزان و مجریان استقرار و توسعهٔ ملّی اطلاعات به شمار آمده تا با دسترسی سریع مدیران راهبردی کشور به اطلاعات صحیح و دقیق، بتوانند به گزینه‌های مناسب تصمیم‌گیری متصل و همسو با منافع امنیت ملّی به صورت یکپارچه گام بردارند.

سیفی پاسندی (۱۳۹۷) در مقاله اشراف اطلاعاتی درفضای مجازی در افق ۱۴۰۴ عنوان نموده که اشراف اطلاعاتی، مؤلفه‌ای است که هر یک از طرفین رقابت و در تعامل با درگیری، تلاش می‌کنند تا زودتر به آن دست یابند و مدت بیش‌تری این اشراف را حفظ کنند و بر دامنه و ابعاد آن بیفزایند. در سال ۱۴۰۴ شمسی یک ربع قرن از قرن بیست و یکم میلادی گذشته و با گسترش دامنه حضور و نقش آفرینی رایانه ها و شبکه های رایانه‌ای و ظهور نسل‌های پیشرفته تر این تجهیزات، فضای حاکم بر ارتباطات، تعاملات و رقابت ها در جوامع بشری، بیش‌تر از آنکه بر جنبه‌های عینی و فیزیکی مستقر باشند، بر فضای مجازی استوار خواهند بود. بنابراین فضای مجازی در همه جنبه‌های زندگی بشری، نقش محوری را بر عهده خواهد داشت. در عصر فضای مجازی، برتری و سرعت عمل در شناخت محیط (اعم از صحنه رقابت و وضعیت طرفین حاضر در این صحنه)، تصمیم‌گیری و برنامه‌ریزی (اعم از چرخه جمع‌آوری داده‌های اولیه، تولید و برون‌دادها و بازخوردگیری)، عمل و اقدام (اعم از فعال یا منفعل، آفندی یا پدافندی) بیش از حال

حاضر، تأثیرگذار و مزیت آفرین خواهد بود. در عصر فضای مجازی، تلفیق و ترکیب هوش انسانی با هوش ابزاری (رایانه‌ها) محوری‌ترین مؤلفه تعیین‌کننده در توانمندی‌های بالقوه و بالفعل طرفین حاضر در صحنه عنوان گردیده است. در ادامه پیشنیه تحقیقات مرتبط با موضوع در قالب جدول شماره ۱ ارائه شده است.

جدول ۱– مرور ادبیات و پیشینه موضوع پژوهش

موضوع پژوهش/ مقاله	نویسنده / نویسندگان	خلاصه و نتایج پژوهش
چالش‌ها و راهکارهای اشرافیت اطلاعاتی در فضای سایبر	بابک اسماعیلی (۱۳۹۵)	برای تشکیل بستر حضور ابزارهای اشرافیت بر فضای سایبری و برای ورود به این فضا نیاز است تا سازمان اطلاعاتی پلیس ابتدا خود را اسکن نموده و در توصیف خود، مشکلات و چالش‌های خود را رؤیت نماید. حضور در فضای سایبری با سخنرانی و تشکیل جلسات متعدد و کلیشه‌ای خالی از آگاهی در مورد خود و این فضا و گماشتن مدیران غیرمتخصص بر بخش‌های تخصصی، نمی‌تواند چاره‌ساز مشکلات، برای حضور و مقابله با تهدیدات فضای سایبری باشد. از این رو شناخت خود و ناتوانی‌ها و توانایی و رفع نواقص و تقویت دانسته‌ها در مورد این فضا می‌تواند متضمن حضوری موفق و کارا باشد.
طراحی الگوی کاربردی برای تحقق اشراف اطلاعاتی در سازمان‌های حفاظت اطلاعات (با تأکید بر فرامین تدابیر فرماندهی معظم کل قوا (مدظله‌العالی))	ابوالفضل پورمنافی (۱۳۹۶)	از تحقیق این نتیجه حاصل می‌گردد که در مفهوم اشراف اطلاعاتی به دو نوع اشراف اطلاعاتی کلی و اشراف اطلاعاتی جزئی برخورد می‌نماییم. اشراف اطلاعاتی کلی به مثابه زنجیره‌ای است که هر حلقه آن بخشی از اشراف بوده و تمامی حلقه‌ها، هر یک، جزئی از اشراف کلی را تشکیل می‌دهند. اولین و مهم‌ترین گام در خصوص پیشگیری تهدیدها و آسیب‌پذیری‌های اشراف اطلاعاتی در سازمان‌های حفاظت اطلاعات، آگاه‌سازی اصولی و به موقع کارکنان حفاظت‌هاست. این الگو اصول کلی در قالب فرامین و تدابیر از ناحیهٔ فرماندهٔ صاحب ولایت و حسب اقتضائات زمان و مکان بوده و در نگاه کلان سه فازی بودن تحقق اشراف اطلاعاتی در سازمان‌های حفاظت اطلاعات را بیان داشته و تحلیل راهبردی را حاکم دائمی و مستمر بر هر لحظه از این الگو قلمداد می‌نماید.
نقش هادی عملیات جمع‌آوری پنهان در اشراف اطلاعاتی سازمان‌های اطلاعاتی –امنیتی	رحیم یعقوبی (۱۳۹۲)	نتایج مؤید آن است که هادی عملیات جمع‌آوری پنهان، نقش‌هایی چون هدایت، تأمین نیازمندی‌های خبری - اطلاعاتی، ارتباطات، آموزش، کمک به پیش‌بینی اطلاعاتی (برآورد تهدیدات) و کمک به تولید فرصت در اشراف اطلاعاتی سازمان‌های اطلاعاتی - امنیتی ایفا می‌نماید.

موضوع پژوهش/ مقاله	نویسنده / نویسندگان	خلاصه و نتایج پژوهش
طراحی الگوی راهبردی اشراف اطلاعاتی کارآمد	احمد چراغی (۱۳۹۷)	هشداردهی، روندی است که از آینده‌نگری و آینده‌شناسی آغاز می‌شود و طی آن، انواع حالات ممکن و محتمل شناسایی و برای هر حالت و احتمال، نشان‌ها و علاماتی در نظر گرفته می‌شود. در نهایت، رصد و پایش شاخص‌های هشدار مطمع نظر قرار می‌گیرد. محصول نهایی هشداردهی، تعیین شکاف یا فاصله میان وضع موجود پدیده با پیش‌بینی‌های قبلی است که البته، ممکن است منجر به شکل‌گیری سناریوها یا پیش‌بینی‌های جدید نیز بشود.

اشراف اطلاعاتی سایبرمحور: نتیجه یک فعالیت جامع، منطقی و مداوم و مبتنی بر یک منطق اطلاعاتی و امنیتی در حوزه فضای سایبر است که می‌تواند شناخت موردنیاز سازمان را به منظور نیل به امنیت و آرامش جامعه فراهم نماید. اشراف اطلاعاتی در فضای سایبر منجر به افزایش سرعت در شناخت محیط، تقویت توان تصمیم‌گیری، اقدام و افزایش هوشیاری اطلاعاتی نسبت به چالش‌ها و تهدیدات سایبری می گردد.

اصول اشراف اطلاعاتی: اصول اشراف اطلاعاتی، قواعد پایداری هستند که حاکم بر تلاش سازمان‌های اطلاعاتی است که از طریق به کارگیری این اصول، شالوده کار اطلاعاتی، مفهوم خاص پیدا می کند و در صورت عدم رعایت این اصول، موجودیت سازمان اطلاعاتی در معرض خطر قرار گرفته و از دستیابی به اهداف مورد نظر باز خواهد ماند. این اصول عبارتند از:

الف-اصل پنهان کاری: پنهان کاری عبارت است از انجام هر فعل یا ترک فعلی که به منظور پوشیده نگه داشتن هویت عوامل اطلاعاتی و مأموریت‌های واگذاری و... انجام می‌شود.

ب-اصل نیازمندی اطلاعاتی: نقطه آغاز کار اطلاعاتی، تعیین نیازمندی خبری و اطلاعات است. تمام سازمان‌های اطلاعاتی با تمام سازوکارهای خود در انجام وظایف و مأموریت خود، نیاز به اطلاعات داشته و تلاش می‌نمایند تا در حوزه قلمرو کاری خود، اشراف اطلاعاتی داشته باشند.

پ-فرآیند تلاش اطلاعاتی: در فرآیند تلاش اطلاعاتی، بخش‌های ذی‌ربط وظیفه تأمین اخبار و اطلاعات را بر اساس نیازمندی‌های درخواست شده از سوی سازمان‌ها و بخش‌های درخواست کننده، بر عهده دارند.

ت- فرآیند بررسی یا توسعه اطلاعاتی: در فرایند بررسی یا توسعه اطلاعاتی، درخواست کنندگان، پس از دریافت گزارش اطلاعاتی از بخش های جمع آوری، نسبت به تعیین ماهیت اخبار و اطلاعات دریافتی اقدام خواهند نمود. در نگاهی کلی نسبت به هر دو فعالیت تلاش جمع آوری و بررسی اطلاعاتی، در

خواهیم یافت که اساساً اهداف هر دو سازمان حول محور مأموریت سازمانی شکل گرفته و به عبارتی هر دو مجموعه به دنبال یک هدف، یعنی اشراف اطلاعاتی می باشند. (تراپاینت و دیگران:۴).

رویکردهای اشراف اطلاعاتی

در بررسی رویکردها و گرایش حفاظت‌اطلاعاتی جهت نیل به اشراف می‌توان به پنج رویکرد کلی به شرح ذیل اشاره نمود:

رویکرد سیاستی: در این رویکرد بر مبنای سیاست‌گذاری و خط مشی‌گذاری اشراف‌اطلاعاتی در فرایند کسب اخبار و اطلاعات موردنیاز است که عمدتاً دو سیاست را در سرلوحه کار خود قرار می‌دهند که عبارت است از:

۱) سیاست اشراف اطلاعاتی کمّی (جمع‌آوری انبوه)

۲) سیاست اشراف اطلاعاتی کیفی (جمع‌آوری تخصصی) (مطالعه گروهی طرح جامع اشراف ملی اطلاعاتی،۱۳۹۱).

رویکرد روشی: در این رویکرد بر مبنای روش‌های جمع‌آوری اخبار و اطلاعات و به تعبیری عملیات کسب اخبار و اطلاعات موردنیاز یک سازمان اطلاعاتی در سرلوحه کاری خود قرار می‌گیرد. به‌طورکلی اشراف‌اطلاعاتی برای تأمین نیازمندی‌های خود در اهداف موردنظر، با اتخاذ بهترین شگردها و روش‌های مؤثر و کارآمد درصدد تهیه و کسب اخبار و اطلاعات موردنیاز خود برمی‌آید و با فراهم آوردن سازوکارهای مناسب به فراخور هر روشی که امکان دستیابی به اخبار و اطلاعات را با سرعت، صحّت و اطمینان لازم در اهداف اطلاعاتی میسّر نماید، عملیات جمع‌آوری را محقق می‌سازد (مطالعه گروهی طرح جامع اشراف ملی اطلاعاتی،۱۳۹۱).

رویکرد ابزاری: لازمه تحقق اشراف اطلاعاتی وجود یک عنصر مهم دیگر است که به‌عنوان «منبع اطلاعاتی» خوانده می‌شود. این عنصر که از ارکان جمع‌آوری اخبار و اطلاعات به‌حساب می‌آید تحت عنوان «منابع جمع‌آوری» از آن یاد می‌شود. در حقیقت منابع به‌عنوان ابزار روش جمع‌آوری و نقش مؤثر آن‌ها به‌عنوان چشم و گوش اشراف‌اطلاعاتی محسوب می‌شوند و انتظار سیستم جمع‌آوری اخبار و اطلاعات این است که منابع، گزارش مشاهدات خود را در اهداف تعیین‌شده به‌موقع ارائه نمایند. منبع در اصطلاح اطلاعاتی به فرد یا شیءای اطلاق می‌شود که اخبار و اطلاعات موردنیاز سازمان اطلاعاتی را تأمین نموده و به تعبیر وظیفه منابع خبری، کسب اخبار، اطلاعات موردنیاز طرح اشراف در اهداف اطلاعاتی به‌کارگیری شده است و نقش مستقیمی در تأمین نیازمندی‌های اطلاعاتی (محورهای خبری) دارند. اهمیت و نقش منابع جمع‌آوری اخبار و اطلاعات برای اشراف اطلاعاتی همان‌طور که اشاره شد، همانند اهمیّت چشم و گوش در بدن انسان است. اگر بخواهیم به سیره علوی در صدر اسلام مراجعه کنیم در خطبه معروف حضرت

علی علیه‌السلام خطاب به مالک‌اشتر، منابع خبری تحت عنوان عیون نامیده شده است: قال امام علی علیه‌السلام: وابعَث العُیونَ مِن أهلِ الصِّدقِ و الوَفاء علیهِم. برانگیز چشم‌هایی که از اهل راستی بوده و وفای به عهد داشته باشند (مطالعه گروهی طرح جامع اشراف ملی اطلاعاتی،۱۳۹۱).

رویکرد موضوعی: این رویکرد بر مبنای موضوعات و محورهای جمع‌آوری اخبار و اطلاعات موردنیاز و به تعبیر نیازمندی‌های اطلاعات معطوف گردیده و تمام فعالیت‌های جمع‌آوری برای تأمین این نیازمندی‌ها انجام می‌پذیرد. در حقیقت نیازمندی اطلاعاتی مبنای کار دستگاه‌های جمع‌آوری برای ایجاد اشرافیت اطلاعاتی در اهداف موردنظر است. لذا تمامی سازمان‌های اطلاعاتی برای این منظور فعالیت جمع‌آوری خود را بر اساس طرح نیازمندی مشخص می‌نمایند. نیازمندی اطلاعاتی عبارت است از تعیین عناوین موضوعات اطلاعاتی موردنیاز یک سازمان و اولویت‌بندی آن‌ها در جهت نیل به هدف‌های موردنظر. به تعبیری دیگر طرح نیازمندی‌های اطلاعاتی همان تعیین محورهای جمع‌آوری است که بایستی با دقت و مهارت لازم، این محورها و موضوعات مشخص‌شده و به‌عنوان یک راهنمای موضوعی در اختیار کلیه متصدیان و عوامل جمع‌آوری قرار گیرد (مطالعه گروهی طرح جامع اشراف ملی اطلاعاتی،۱۳۹۱).

رویکرد محیطی: در این رویکرد مبانی اشراف اطلاعاتی بر اساس اهداف اطلاعاتی و یا به عبارتی محیط‌های کسب اخبار و اطلاعات موردنیاز در نظر گرفته می‌شود. «هدف» در اصطلاح اطلاعاتی، محل، شخص، تشکیلات یا مجموعه‌ای است که موضوع فعالیت اطلاعاتی قرار می‌گیرد و یا به تعبیری «هدف» عبارت است از محدوده فیزیکی، گروه یا سوژه اطلاعاتی که سازمان اطلاعاتی برای تأمین نیازمندی‌های خبری خود در مورد آن اقدام به جمع‌آوری اخبار و اطلاعات می‌کند. بنابراین حوزه قلمرو فعالیت جمع‌آوری اخبار و اطلاعات و اشراف اطلاعات معطوف به اهداف اطلاعات است و حریم و حیطه جمع‌آوری بر اساس «اهداف» موردنظر تعیین می‌شود و با شناخت دقیق هدف، محورهای جمع‌آوری و نیازمندی اطلاعاتی مشخص گردیده و تمام سازوکارهای جمع‌آوری اعم از اتخاذ روش انتخاب منابع متناسب بر اساس آن تعیین می‌گردد (مطالعه گروهی طرح جامع اشراف ملی اطلاعاتی،۱۳۹۱).

الزامات نیل به اشراف اطلاعاتی سایبر محور

حضور در این فضای سایبر و تلاش برای کسب اشراف اطلاعاتی در آن، نیازمند درک الزامات و ضروریات مربوط به فضای سایبر و پذیرش قواعد و ضوابط حاکم بر آن است که توجه به آن‌ها موجب ارتقاء توانمندی‌ها و افزایش تأثیر اقدامات آفندی و پدآفندی خواهد گردید و عدم توجه لازم و کافی به این ضروریات، به معنای چشم‌پوشی از فرصت‌های ارزشمند و واگذاری این عرصه به دشمنان بوده و امری غیرعقلایی به‌شمار می‌آید. برخی از این ضروریات و الزامات عبارت‌اند از:

– دارا بودن برتری بر دشمن در زمینه سرعت در شناخت محیط، تصمیم‌گیری و اقدام. دنیای آینده بیش‌تر از امروزه بر سرعت متکی خواهد بود و کسب موضع برتر و تأثیرگذارتر در فضای سایبر، منوط به داشتن

سرعت بیش‌تری نسبت به رقبا در تهیه اطلاعات موردنیاز، تبدیل آن به دانش و اتخاذ تصمیمات برتر است.

– فضای سایبر، فضا و محیط نوینی است که نیازمند راهبردها، طراحی‌ها و ساختارهایی متناسب با خود است.

– نقاط قوت و ضعف کشورها در فضای سایبر، با سطح توسعه‌یافتگی آن‌ها رابطه مستقیم دارد.

– جبران شکاف حاصل از تفاوت میزان دسترسی نیروهای نظامی (به‌عنوان بخشی از هر کشور) به علوم، فنون، ابزار و تجهیزات حضور و جنگ در فضای سایبر، بسیار دشوارتر از دیگر ابعاد اختلاف سطح نیروهای نظامی است.

– فضای سایبر قادر است مؤلفه‌ها و متغیرهای مؤثر بر جنگ را به چالش کشیده و آن‌ها را تقویت نموده و یا به چالش جدی بکشاند. بایستی این نکته را مد نظر قرار داشت که تهدیدات سایبری دارای رده های مختلف هستند. تهدیدات علیه زیرساخت اینترنت، تهدیدها علیه تک تک شبکه ها یا سرورها و تهدیدها علیه زیرساخت های حساس. متناسب با هر سطح تهدید بایست شناخت و توانمندی لازم ایجاد شود.

– خودباوری و جلوگیری از ایجاد حالت خودباختگی در نزد کارشناسان و متخصصین خودی در زمینه توان مقابله با دشمن امری ضروری به‌شمار می‌آید.

– هر نیرویی که در فضای سایبر حضور می‌یابد، باید به آسیب‌پذیر بودن دشمن و وجود شکاف‌های متعدد در سازوکارهای موجود در شبکه‌های رایانه‌ای آن‌ها باور داشته باشد. این امر افزایش ضریب اعتماد به نفس نیروهای خودی و افزایش میزان موفقیت آن‌ها در روند اقدامات مربوط به فضای سایبر را به‌دنبال خواهد داشت.

– لزوم بهره‌برداری مؤثر از نیروی عظیم (بالفعل و بالقوه) دانش نرم‌افزاری موجود در تمام سطوح جامعه و مهم‌تر از آن ساماندهی و هدایت مناسب این توانمندی‌ها در راستای اهداف موردنظر.

– کسب قابلیت لازم برای استفاده به موقع، نظام‌مند و هدف‌مند از فرصت‌های بالقوه و بالفعل موجود در محیط سایبر. به‌طور مثال با توجه به این‌که اغلب واحدها و یگان‌های نظامی کشورهای غربی و همچنین نظامیان شاغل در این واحدها، دارای سایت اینترنتی و یا وبلاگ مستقل بوده و بخشی از اخبار و اطلاعات مربوط به کارکنان، خانواده‌های آن‌ها و خود واحدها در این سایت‌ها و وبلاگ‌ها منعکس می‌شوند، و از سوی دیگر بسیاری از نظامیان (به ویژه نظامیان کشورهای غربی) از پست الکترونیکی و ابزارهای مشابه برای برقراری ارتباط با یکدیگر و با بستگان خویش استفاده می‌کنند، شناسایی و جمع‌آوری آدرس‌های این سایت‌ها، وبلاگ‌ها و پست‌های الکترونیکی، می‌تواند در اقدامات آفندی، از جمله موارد

ذیل مورد استفاده قرار گیرند:

- جمع‌آوری اخبار و اطلاعات.
- انجام عملیات هک علیه سایت‌های وابسته به دشمن در هنگام ضرورت.
- انتشار اخبار هدفمند و اطلاعات موردنظر بر روی بخش‌های نظرسنجی و نظرات مخاطبین سایت‌ها و وبلاگ‌های فوق.
- طراحی و ایجاد سایت‌ها و وبلاگ‌های مشابه برای گمراه کردن مخاطبین سایت‌ها و وبلاگ‌های فوق.
- ارسال اخبار هدفمند به پست‌های الکترونیکی نظامیان کشور موردنظر و یا بستگان آن‌ها به منظور ایجاد فضای ناامن روانی در نزد آن‌ها.
- برخورداری از توان استفاده از فرصت‌های خاص.

با توجه به‌وجود متخصصان رایانه‌ای آزاد و غیردولتی در کشورهایی مانند هندوستان، صربستان و اغلب کشورهای بلوک شرق (سابق) که حاضر هستند در ازای دریافت پول، اقدامات تخریبی را علیه سایت‌های موردنظر کارفرمای خویش انجام دهند، می‌توان با استفاده از پوشش‌های مناسب، افراد مجربی را به استخدام درآورده و برای انجام اقداماتی مانند تخریب سایت‌های عملیات روانی دشمن، از آن‌ها استفاده نمود. طبق گزارش پنتاگون، قبل از حمله آمریکا به عراق در سال ۱۹۹۱، گروهی از برنامه‌نویسان بلغاری به صدام پیشنهاد نمودند که حاضر هستند در قبال یک میلیون دلار برنامه‌ای را برای ایجاد اختلال در برنامه‌های مربوط به گسترش نیروهای آمریکا در خاورمیانه را طراحی و اجراء نمایند. صدام این پیشنهاد را قبول نکرد ولی پنتاگون میزان تبعات این تهدید را بالا ارزیابی‌نمود (سیفی پاسندی،۱۳۹۷: ۱۵۰).

طرح‌واره کلی یافته‌های پژوهش

در این بخش طرح‌واره یافته‌های پژوهش که مبتنی بر مؤلفه‌ها، پیامدها و الزامات اشراف اطلاعاتی سایبرمحور است، ارائه می گردد. برای دستیابی به پایه‌های اصلی این طرح‌واره با انجام مصاحبه با تعداد ۸ نفر از نخبگان و بررسی آثار و ادبیات موجود در حوزه اشراف اطلاعاتی و فضای سایبر، در نهایت مشخص گردید که ۳ مفهوم درک سایبری، فهم سایبری و تجسم سایبری از مؤلفه‌های اصلی اشراف اطلاعاتی سایبرمحور بوده که هر یک دارای ابعاد و ویژگی‌های خاص خود می‌باشند. در ارتباط با پیامدهای اشراف اطلاعاتی سایبر محور نیز تعداد ۴ مفهوم شامل برتری عملیاتی، پیشگیری از غافلگیری، خنثی‌سازی و ارتقاء امنیت سایبری شناسایی گردید و در نهایت به منظور نیل به اشراف اطلاعاتی سایبرمحور سازمان‌های اطلاعاتی و امنیتی باید الزامات زیر را در دستور کار خود قرار دهند که عبارت اند از: تاثیر دانش سایبری در اشراف اطلاعاتی سایبرمحور، تاثیر مهارت در اشراف اطلاعاتی سایبرمحور، وجود زیرساخت‌های مناسب، نیروی انسانی متخصص، تاثیر نظامات سایبری در اشراف اطلاعاتی سایبرمحور، دستورالعمل‌ها و آیین‌نامه‌ها.

ابعاد	مؤلفه‌ها	ابعاد
اشراف اطلاعاتی سایبرمحور در سازمان های اطلاعاتی و امنیتی	درک سایبری (جمع‌آوری)	دسترسی به گلوگاه‌های سایبری کشور
		گسترش شبکه‌های جمع‌آوری
		تاثیر مهندسی اجتماعی در اشراف اطلاعاتی سایبرمحور
		تاثیر مراقبت در اشراف اطلاعاتی سایبرمحور
		پایش فعالیت‌های کاربران
		سامانه‌های کاوشگر و جست‌وجوگر هوشمند
		اشتراک اطلاعات (تبادل اطلاعات بین سازمانی)
		زمان روی دادن اتفاقات
		کنترل های لازم برای تشخیص دادن رویدادها
		تاثیر تشخیص هویت در اشراف اطلاعاتی سایبرمحور
	فهم سایبری (تحلیل)	تجمیع بانک‌های اطلاعاتی (یکپارچگی اطلاعات)
		طبقه‌بندی اطلاعات
		پرورش تفکر انتقادی
		هوش مصنوعی و داده‌کاوی
		ادغام قابلیت‌های اطلاعاتی
		تکنیک‌های تحلیل
		فرآیند تحلیل
	تجسّم (ترسیم) سایبری	شناخت روندهای سایبری
		توانایی پیش‌بینی آینده (بر اساس دانش احصائی از دینامیک عناصر و درک وضعیت)
		شبیه‌سازی
		تفسیر و سنتز (ترکیب و مرتبط کردن شواهد و داده‌ها)
		توجه به معانی ضمنی وضعیت درک شده
		ترکیب فازی مؤلفه‌های رفتار، قابلیت و نیّت

بررسی پیامدها	پیامدهای اشراف اطلاعاتی سایبرمحور	برتری عملیاتی
		پیشگیری از غافلگیری
		خنثی سازی
		ارتقاء امنیت سایبری
زمینه‌سازها و الزامات	الزامات اشراف اطلاعاتی سایبرمحور	تاثیر دانش سایبری در اشراف اطلاعاتی سایبرمحور
		تاثیر مهارت در اشراف اطلاعاتی سایبرمحور
		وجود زیرساخت‌های مناسب
		نیروی انسانی متخصص
		تاثیر نظامات سایبری در اشراف اطلاعاتی سایبرمحور
		دستورالعمل‌ها و آیین‌نامه‌ها

یافته های پژوهش

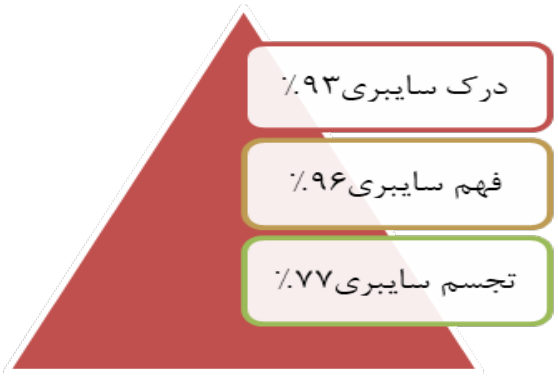
روش تجزیه و تحلیل داده‌ها: در این پژوهش ابزار جمع‌آوری اطلاعات پیرامون ادبیات و مبانی نظری از راه مطالعه کتابخانه‌ای و در بخش میدانی، از طریق مصاحبه عمقی و توزیع پرسشنامه صورت گرفت. در بخش مصاحبه، تعداد ۳ سؤال اصلی متناسب با سؤالات پژوهش و یک سؤال تحت عنوان پیشنهادها طرح و پس از چند مرحله اخذ نظریه نخبگان جامعه آماری در رابطه اعتبار آن و انجام نظریات اصلاحی، روایی آن محرز شد و سپس با تعداد ۹ نفر از اعضای جامعه آماری مصاحبه به عمل آمد. بر مبنای ادبیات نظری و همچنین نظر مصاحبه‌شوندگان پرسشنامه ۳۶ سؤالی طراحی که روایی آن به دو طریق روایی محتوایی و روایی صوری مورد تأیید قرار گرفته است. روایی محتوایی (زیرمجموعه روایی صوری) که در آن از نظر و دیدگاه صاحب‌نظران در مورد محتوای سؤالات پرسشنامه استفاده می‌شود. در این پژوهش اعتبار پرسشنامه از طریق الفای کرونباخ محاسبه شده که عدد به‌دست‌آمده (۰/۵۷) بیانگر این است که پرسشنامه از اعتبار قابل قبولی برخوردار است. در این پژوهش داده‌ها در بخش کیفی به صورت توصیفی و استنباطی تجزیه و تحلیل شده و در بخش کمی نیز به منظور توصیف داده‌های مذکور از نرم‌افزار spss استفاده شده است.

تجزیه و تحلیل داده‌ها و یافته‌ها

تحلیل نتایج به دست آمده، موارد زیر را نشان داده است:

الف. در مجموع ۹۳ درصد پاسخ‌دهندگان در حد زیاد و خیلی زیاد موافق سازوکارهای مرتبط با درک سایبری (شامل دسترسی به گلوگاه‌های سایبری کشور، گسترش شبکه‌های جمع‌آوری، مهندسی اجتماعی، مراقبت، پایش فعالیت‌های کاربران، بهره‌گیری از سامانه‌های کاوشگر و جست‌وجوگر هوشمند، اشتراک

اطلاعات و...)، ۹۶ درصد پاسخ‌دهندگان در حدّ زیاد و خیلی زیاد موافق سازوکارهای مرتبط با فهم سایبری (از قبیل تجمیع بانک‌های اطلاعاتی، طبقه‌بندی اطلاعات، پرورش تفکر انتقادی، هوش مصنوعی و داده‌کاوی، ادغام قابلیت‌های اطلاعاتی، تکنیک‌های تحلیل، فرآیند تحلیل) و ۷۷ درصد پاسخ‌دهندگان در حد زیاد و خیلی زیاد نسبت به تجسّم سایبری (شامل شناخت روندهای سایبری، توانایی پیش‌بینی آینده، شبیه‌سازی، تفسیر و سنتز، توجه به معانی ضمنی وضعیت درک شده و همچنین ترکیب فازی مؤلفه‌های رفتار، قابلیت و نیّت) به عنوان مولفه‌های اشراف اطلاعاتی سایبرمحور نظر مساعد داشته و بهره‌گیری از الزامات دانش، مهارت، زیرساخت‌ها، نیروی‌انسانی متخصص، نظامات سایبری و دستورالعمل‌ها را موجبات فراهم آمدن پیامدهایی از قبیل برتری عملیاتی، پیشگیری از غافلگیری، خنثی‌سازی و ارتقاء امنیت سایبری می‌دانند.



نمودار ۱[۱]

ب.تأثیر درک سایبری (جمع آوری) در اشراف اطلاعاتی سایبرمحور: میانگین‌های رتبه‌ای سؤالات مربوط به تاثیر درک سایبری در اشراف اطلاعاتی سایبرمحور مبین آن است که از بین ده سوال مطرح شده در این حوزه، عامل «کنترل های لازم برای تشخیص دادن رویدادها با (ارزش رتبه‌ای ۷/۵۲) و عامل «زمان روی دادن اتفاقات» (با ارزش رتبه‌ای ۲/۶۵) به ترتیب دارای بیش‌ترین و کم‌ترین تأثیرگذاری بر اشراف اطلاعاتی سایبرمحور هستند.

پ. تأثیر فهم سایبری (تحلیل) در اشراف اطلاعاتی سایبرمحور: میانگین‌های رتبه‌ای سؤالات مربوط به تأثیر فهم سایبری در اشراف اطلاعاتی سایبرمحور مبیّن آن است که از بین هفت سوال مطرح شده در این حوزه، عامل «تکنیک‌های تحلیل» (با ارزش رتبه‌ای ۵/۵۵) و عامل «فرایند تحلیل» (با ارزش رتبه‌ای ۲/۹۹) به ترتیب دارای بیش‌ترین و کم‌ترین تأثیرگذاری بر اشراف اطلاعاتی سایبر محور هستند.

ت.تأثیر تجسم سایبری (ترسیم) در اشراف اطلاعاتی سایبرمحور: میانگین‌های رتبه‌ای سؤالات مربوط به

۱. نمودار مولفه های موثر بر اشراف اطلاعاتی سایبر محور

تأثیر تجسم سایبری در اشراف اطلاعاتی سایبرمحور مبین آن است که از بین شش سوال مطرح شده در این حوزه، عامل «شناخت روندهای سایبری» (با ارزش رتبه‌ای ۴/۳۹) و عامل «توانایی پیش‌بینی آینده بر اساس دانش احصائی از دینامیک عناصر و درک وضعیت (با ارزش رتبه‌ای ۲/۵۹) به ترتیب دارای بیش‌ترین و کم‌ترین تأثیرگذاری بر اشراف اطلاعاتی سایبرمحور هستند.

ج.پیامدهای اشراف اطلاعاتی سایبرمحور: مؤلفه‌های مربوط به پیامدهای اشراف اطلاعاتی دارای میانگین تقریبی ۴/۵ هستند و دارای سطح معناداری صفر (عدد آزمون ۴) است. این نشان‌دهنده این است که افراد جامعه آماری معتقدند اشراف اطلاعاتی پیامدهای خوبی برای سازمان‌های اطلاعاتی و امنیتی در پی خواهد داشت.

چ.الزامات اشراف اطلاعاتی سایبرمحور: مؤلفه‌های مربوط به الزامات اشراف اطلاعاتی دارای میانگین تقریبی ۴ هستند و دارای سطح معناداری صفر (عدد آزمون ۴) است. این نشان دهنده این است که افراد جامعه آماری معتقدند این مؤلفه‌ها تا حد زیادی زمینه‌ساز اشراف اطلاعاتی هستند.

نتیجه گیری

یکی از روش‌های مهم در رسیدن به اشراف و احاطه اطلاعاتی سایبرمحور، اخبار و اطلاعاتی است که از طریق جمع‌آوری سایبری کسب می‌شود. داشتن اطلاعات سایبری پنهان از نیروهای حریف و هدف، اگر چه کاری صعب و پُرهزینه است اما منبعی مهم برای اعمال قدرت است. در رسیدن به اشراف اطلاعاتی سایبرمحور عوامل زیادی دخالت دارند و هر کدام به نحوی تأثیرگذار هستند که در صورت حذف و نادیده گرفتن آن‌ها، این مهم به سرانجام نرسیده یا هزینه‌های زیادی را طلب می‌کند. برای تحقق اشراف اطلاعاتی سه حوزهٔ درک سایبری، فهم سایبری و تجسّم بایستی مدنظر قرار گیرد. این الگو در حوزه درک سایبری با توان دسترسی به گلوگاه‌های سایبری کشور، گسترش شبکه‌های جمع‌آوری، مدنظر قرار دادن مهندسی اجتماعی، مراقبت، پایش فعالیت‌های کاربران، بکارگیری سامانه‌های کاوشگر و جست‌وجوگر هوشمند، اشتراک اطلاعات، ثبت زمان روی دادن اطلاعات، ایجاد کنترل برای تشخیص دادن رویدادها و تشخیص هویت و در حوزه فهم سایبری به وسیله تجمیع بانک‌های اطلاعاتی (یکپارچگی اطلاعات)، طبقه‌بندی اطلاعات، پرورش تفکر انتقادی، بهره‌گیری از هوش مصنوعی و داده‌کاوی، ادغام قابلیت‌های اطلاعاتی، بهره‌گیری از تکنیک‌ها و فرآیند تحلیل و در آخرین حوزه یعنی تجسّم (ترسیم) با مدنظر قرار دادن شناخت روندهای سایبری، توان پیش‌بینی آینده (بر اساس دانش احصائی از دینامیک عناصر و درک وضعیت)، شبیه‌سازی، تفسیر و سنتز (ترکیب و مرتبط کردن شواهد و داده‌ها)، توجه به معانی ضمنی وضعیت درک شده و استفاده از ترکیب فازی مؤلفه‌های رفتار، قابلیت و نیّت می‌تواند موجبات تحقق اشراف اطلاعاتی سایبرمحور را در سازمان‌های اطلاعاتی و امنیتی فراهم آورد.

منابع:

- برقعی، مهدی (۱۳۹۳)، **مروری بر امنیت سایبری**؛ درس هایی برای جمهوری اسلامی ایران، فصلنامه علمی- پژوهشی مطالعات انقلاب اسلامی، سال یازدهم، شماره ۳۸، صص ۸۶-۸۵.
- بیابانی، غلامحسین و اسفندیاری، مسعود (۱۳۹۶)، **اشراف اطلاعاتی در سازمان های پلیسی**، فصلنامه کارآگاه، سال نهم، شماره ۳۹، صص ۴۲-۴۰.
- پاسندی، عین اله (۱۳۹۷)، **اشراف اطلاعاتی در فضای مجازی در افق ۱۴۰۴**، دو فصلنامه علمی مقابله با عملیات روانی، سال سوم، شماره ۵، دانشکده علوم و فنون فارابی ۱۵۰-۱۴۷.
- پورقهرمانی، بابک (۱۳۹۹)، **چالش های امنیت سایبری در کشورهای «آ سه آن»**، فصلنامه مطالعات بین المللی، سال ۱۸، شماره ۱، صص ۱۴۱-۱۳۸.
- پورمنافی، ابوالفضل (۱۳۹۶)، **طراحی الگوی راهبردی اشراف اطلاعاتی ناجا**، دانشگاه پلیس ناجا، تهران، دانشکده امنیت ملی دانشگاه عالی دفاع ملی.
- خواجه امیری، مهدی؛ قاسمی، علی و بابایی، حسین، (۱۳۸۹)، **مبانی اشراف اطلاعاتی**، تهران: معاونت پژوهش دانشگاه فارابی، صص ۳۵-۳۴.
- زابلی زاده، اردشیر و وهاب‌پور، پیمان (تابستان ۱۳۹۷)، **قدرت بازدارندگی در فضای سایبر**، رسانه و فرهنگ، پژوهشگاه علوم انسانی و مطالعات فرهنگی، سال هشتم، شماره اول، ۴۸-۴۶.
- عصاریان‌نژاد، حسین (۱۳۹۱)، **بررسی تحلیلی قابلیت‌های شبکه ای اشراف اطلاعاتی**، تهران، مجله امنیت دفاعی، ۷۸-۷۶.
- محمودزاده، ابراهیم و اسماعیلی، کیوان (زمستان ۱۳۹۷)، **الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح**، فصلنامه امنیت ملی، سال هشتم، شماره سی ام، صص ۲۰۴-۲۰۲.
- مزینانی، احمد (۱۳۹۲)، **اشراف اطلاعاتی**، فصلنامه هادی، دانشکده امام هادی (ع) حفاظت اطلاعات سپاه پاسداران، ۲۲۳-۲۲۱.
- مطالعه گروهی در دانشگاه دفاع ملی، (۱۳۹۳)، **شاخص‌های اشراف ملّی اطلاعات در ارتش جمهوری اسلامی ایران**.
- موسوی، محمد رضا و مستجابی سرهنگی، حمید (تابستان ۱۳۹۲)، **تبیین مفهوم مرز در فضای سایبر**، فصلنامه علمی- ترویجی دانشکده علوم و فنون مرز، سال چهارم، ۲۴-۲۲.
- نجفی، محسن و حسینی، رضا (۱۴۰۰)، **حکمرانی سایبری**، تهران: انتشارات مرکز آموزش شهید صیاد شیرازی.
- وبستر، فرانک (۱۳۸۴)، **نظریه‌های جامعه اطلاعاتی**، ترجمه مهدی داوری، تهران، انتشارات وزارت امورخارجه.

- *Helokunnas,T,Kuusisto,R.* (2003)***Acquiring information superiority by time-divergent communication***.*InProceeding of the2nd European Conference on information Warfare and Securoty(pp.1-9)*
- *Trepant,H,Jansen,M,Lamaa A.* (***Achievind Information superiority Five Iperatives for Military Transformation***),*Strategy and Bozz Co*