فصلنامه تهدید پژوهی
دوره ۱، شماره ۱، شماره پیاپی (۱)، بهار ۱۴۰۲، ص ۱۱۷ ـ ۹۳

چالش‌های اطلاعاتی و امنیتی در عصر اطلاعات

محسن نجفی[۱]، تورج گیوری[۲]

تاریخ دریافت: ۱۴۰۲/۰۱/۱۶ تاریخ پذیرش: ۱۴۰۲/۰۳/۲۲

چکیده:

عصر اطلاعات با ویژگی‌های منحصربه‌فرد خود ظهور کرده است. این عصر در کنار فرصت‌های بی‌شماری که پیش روی جامعه اطلاعاتی قرار داده، تهدیدها و چالش‌هایی را نیز متوجه آن ساخته است. انقلاب اطلاعات و ارتباطات، جوامع صنعتی را به‌سوی اطلاعاتی شدن سوق داده است. در جامعه اطلاعاتی، اطلاعات به عنصری اساسی در حیات جامعه تبدیل‌شده است. در این بستر متغیر، معادلات امنیتی نیز دستخوش تغییرات اساسی شده و عنصر اطلاعات به‌عنوان عنصر نامحسوس قدرت ارزشی ویژه یافته است. تغییرات جدید، تهدیدات و چالش‌های امنیتی جدیدی پدید آورده است. در این نوشتار چالش‌های اطلاعاتی و امنیتی عصر اطلاعات در ابعاد مختلف اعم از چالش‌های امنیت سایبری، اقدام پنهان، اطلاعات آشکار و چالش‌های فراروی چرخه اطلاعات مورد واکاوی قرارگرفته است. نتایج به‌دست‌آمده حاکی از آن است که رشد غیرقابل‌باور فناوری اطلاعات و ارتباطات ابعاد مختلف مأموریت سازمان‌های اطلاعاتی و امنیتی را با چالش‌هایی عمده روبه‌رو ساخته است و ضرورت تغییر در مدیریت سازمان‌های اطلاعاتی و امنیتی و تناسب با تغییرات جدید بیش‌ازپیش احساس می‌گردد.

واژگان اصلی: اطلاعات، عصر اطلاعات، سازمان‌های اطلاعاتی.

۱. دانش آموخته دکتری علوم سیاسی دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران، ایران (نویسنده مسئول)
۲. دانش آموخته دکتری علوم سیاسی دانشگاه آزاد اسلامی واحد تهران شمال، تهران، ایران

مقدمه

گفتمان نوین امنیت در عصر ما بیانگر این حقیقت تلخ است که همگام با پیشرفت بشر در عرصه‌های گوناگون مؤلفه‌های ناامنی نیز وسعت یافته است و درنتیجه انسان معاصر با ناامنی بیش‌تری روبه‌رو است. احتمال تجاوز از سوی دولت‌ها، گروه‌ها، افراد و یا ترکیبی از آن‌ها وجود دارد. متجاوزان به‌صورت ناشناسی وارد عمل می‌شوند. درصورتی‌که شاید حتی به‌طور فیزیکی به کشور نزدیک هم نشده باشند. شکل ارتباطات تغییر کرده است و برقراری ارتباط فرد با فرد، فرد با جمع، جمع با فرد و از همه مهم‌تر جمع با جمع به‌راحتی و با سرعتی بالا تحقق می‌یابند. ارتباطات غیرمتمرکز قدرت کنترل مرکزی محدودشده است. عصر اطلاعات با ویژگی‌های منحصربه‌فرد خود ظهور کرده است. این عصر در کنار فرصت‌های بی‌شماری که پیش روی جامعه اطلاعاتی قرار داده، تهدیدها و چالش‌هایی را نیز متوجه آن ساخته است. انقلاب اطلاعات و ارتباطات، جوامع صنعتی را به‌سوی اطلاعاتی شدن سوق داده است. در جامعه اطلاعاتی، اطلاعات به عنصری اساسی در حیات جامعه تبدیل‌شده است. در این بستر متغیر، معادلات امنیتی نیز دستخوش تغییرات اساسی شده و عنصر اطلاعات به‌عنوان عنصر نامحسوس قدرت ارزشی ویژه یافته است. تغییرات جدید، تهدیدات امنیتی جدیدی را در گفتمان امنیت ملی کشورها مطرح می‌سازد. تهدیدات جدید، ماهیت اطلاعاتی دارد و استراتژی‌های مقابله‌ای ویژه‌ای را می‌طلبد. (شریف،۱۳۸۷:۱۲۳) زمانی تهدید صرفاً در شکل خارجی و بیرونی آن تحلیل می‌شد و هر نوع خطری که از بیرون مرزهای سیاسی متوجه نظام سیاسی می‌شد، به‌عنوان تهدید در نظر گرفته می‌شد، اما با پیشرفت جوامع بشری و تغییر در شکل روابط، شکل تهدید نیز دگرگون شد تا جایی که امروزه، با توسعه مطالعات امنیتی، بعد داخلی به‌عنوان مهم‌ترین بعد تهدید تحلیل می‌شود. ازاین‌رو، در رویکردهای داخلی، عمدتاً ابعاد جامعه‌شناختی موضوع تحلیل می‌شود و همه گروه‌هایی که در حوزه داخلی کار می‌کنند، در بحث‌های امنیتی و غیرامنیتی که در مقام تجزیه‌وتحلیل پدیده‌های داخلی هستند، لاجرم از زاویه جامعه‌شناسی به تحلیل موضوع می‌پردازند. به همین نسبت، سازمان‌های اطلاعاتی نیز از وظایف جدیدی در حوزه‌های بررسی، اقدام پنهان، جمع‌آوری و حفاظت برخوردار شده‌اند. (قاضی‌زاده،۱۳۹۲:٤٠) ازاین‌رو ضروری است تا سازمان‌های اطلاعاتی، چالش‌های جدید اطلاعاتی و امنیتی را شناسایی و متناسب با آن به اتخاذ تدابیر مقابله‌ای بپردازند.

بیان مسئله:

سرویس‌های اطلاعاتی – امنیتی اجزای اصلی و کلیدی هر دولتی به شمار می‌روند، زیرا تحلیلی مستقل از اطلاعات مربوط به امنیت داخلی و خارجی دولت، جامعه و حفاظت از منافع حیاتی ملت فراهم می‌آورند. بخش اطلاعات هر کشور حوزه خاصی از فعالیت‌های دولتی است که نقش مهمی در تضمین امنیت بر عهده دارد. (افتخاری و قدرت‌آبادی،۱۳۹۵:۲٤) انقلاب اطلاعات شاید هیچ بخشی از بروکراسی دولتی را به‌اندازه سازمان‌های اطلاعاتی و سپس ساختار نظامی دست‌خوش تغییر و دگرگونی نساخته باشد. دلیل این امر تا حدود بسیاری مشخص است. زیرا حیات و کارکرد دستگاه‌های اطلاعاتی وابسته به اطلاعات است و حال چگونه می‌شود چرخه‌های اطلاعاتی در جوامع تغییرات اساسی را تجربه کنند اما سازمان‌های اطلاعاتی از آن متأثر نشوند. از طرف دیگر آنچه حجم و گستره این تأثیرپذیری را بیشتر ساخت، هم‌زمانی نسبی انقلاب اطلاعات با تغییر راهبردی جهانی به‌واسطه تغییر نظم جهانی ناشی از فروپاشی اتحاد جماهیر شوروی است. هم‌زمانی این دو رخداد با یکدیگر، یعنی تغییر نظم بین‌المللی و انقلاب اطلاعاتی، مباحثات گسترده‌ای را در دستگاه‌های اطلاعاتی کشورها برای ایجاد تغییرات ساختاری برپا کرد. (دیو سالار،۱۳۹٤:۹۰) محیط عصر اطلاعات ویژگی‌های متفاوتی از گذشته دارد و مؤلفه‌های ماهیت غیر تحمیلی و غیرنظامی گردش اطلاعات، ارسال چندرسانه‌ای اطلاعات، شبکه‌ای شدن اطلاعات، پنهان بودن چهره سیاست در گردش اطلاعات، چهار تغییر عمده را در محیط راهبردی ایجاد نموده است که عبارت‌اند از؛ برتری نخبگان اطلاعاتی، امکان بازگیری قدرت‌های کوچک، فشردگی زمان و مکان، هویت محوری. از ویژگی‌های بارز عصر اطلاعات می‌توان به فقدان انسجام معنایی، تضعیف سامانه ایمنی و دفاعی ذهنی در برابر تهاجم اطلاعات، بی‌تفاوتی و گریز از اخبار به سبب انبوه اخبار و اطلاعات اشاره کرد. عصر اطلاعات، راهبردهای نظامی، ساختارهای سازمانی، آموزه‌ها و سیاست‌های دفاعی را تغییر داده و مفاهیم نوینی از جنگ اطلاعاتی را پدید آورده است. لذا امروزه کشورهای بسیاری به دنبال کسب توانایی اجرای حملات اطلاعاتی در سطح راهبردی هستند. دغدغه اصلی نویسنده در این نوشتار شناخت چالش‌های اطلاعاتی و امنیتی در عصر اطلاعات باهدف اتخاذ سیاست‌های پیشگیرانه و مقابله‌ای متناسب می‌باشد.

ادبیات تحقیق

اطلاعات

اطلاعات را در بهترین شکل می‌توان چنین تعریف کرد:"اخبار جمع‌آوری‌شده، سازمان‌دهی شده یا تجزیه‌وتحلیل شده از طرف بازیگران یا سیاست‌گذاران." جفری. تی.ریچلسون اطلاعات را چنین تعریف می‌کند:"محصولی که از جمع‌آوری، ارزیابی، تجزیه و ترکیب و تفسیر تمام اخبار موجود به دست می‌آید و به‌نوعی در ارتباط با ملل خارجی یا مناطق عملیاتی است که در حال حاضر برای برنامه‌ریزی مهم است یا می‌تواند در آینده برای برنامه‌ریزی مهم باشد". رابرت بوی نیز به‌نوبه خود اطلاعات را خیلی ساده و ظریف، چنین تعریف می‌کند:"اطلاعات عبارت است از اخباری که برای اقدام (عملیات) طراحی‌شده است"(گادسون و همکاران،۱۳۸٤:۲۹)

سازمان‌های اطلاعاتی

سازمان‌های اطلاعاتی را می‌توان بخشی از ساختار اداری دولت مدرن دانست که به‌واسطه کارکردشان تعریف و شناخته می‌شوند. این سازمان‌ها وظیفه حساس و مهم گردآوری، تحلیل و مدیریت اطلاعات حاصله از ابعاد آشکار و پنهان پدیده‌ها را بر عهده‌دارند و از این حیث در ایجاد شناخت واقعی و جامع از محیط داخلی و پیرامونی برای سیاست‌گذاران نقش اساسی دارند. به همین دلیل است که سازمان‌های اطلاعاتی در تمامی دولت‌ها دارای اهمیت و حساسیت بالایی می‌باشند و در تأمین منافع و صیانت از امنیت، نقش محوری دارند. (پیرمحمدی،۱۳۹۰:۳۸).

عصر اطلاعات

عصر اطلاعات را حاصل سومین انقلاب اجتماعی، پس از انقلاب کشاورزی و انقلاب صنعتی دانسته‌اند. به تعبیر بیل کولمن، انقلاب اطلاعات، سومین انقلاب اقتصادی است. به اعتقاد وی انقلاب کشاورزی با مقدار غذای قابل تولید برای تغذیه جمعیت سروکار داشت. میزان و سرعت انتقال سرمایه نیز برانگیزاننده و هموار کننده انقلاب اقتصادی بود و آنچه موجب تغییر امروز جهان است، افزایش شگفت انگیز مقدار و سرعت انتقال اطلاعات است. برجسته‌ترین مشخصه عصر اطلاعات، رشد فناوری‌ها و به ویژه فناوری‌های اطلاعات و ارتباطات و فراگیر شدن آن در سطح جهان است که اصلی‌ترین محرکه پویایی در این عصر می‌باشد. (گنجی دوست،۱۳۸۷:۱۹۱) عصر اطلاعات دارای ویژگی‌هایی شامل کاهش فاصله جغرافیایی و زمانی، تغییر بنیادین در نحوه تولید ثروت، تحول در مفاهیم و شاخص‌های اقتصادی، اجتماعی، مدیریتی و

سازمان‌دهی، تغییر مؤلفه قدرت سیاسی حکومت‌ها، افزایش چشم گیر پیچیدگی در مسائل جهـانی، سـرعت بـه‌عنوان اسـتراتژی حرکـت و تبـدیل شـدن اطلاعـات بـه کـالا می‌باشـد. (زارعـی و واحدی،۱۳۸٦:۸۳)

مراحل تکاملی اطلاعات محرمانه

در نگاهی به گذشته اطلاعات محرمانه مدرن، سه دوره متفاوت ظهور می‌کنند؛ ایـن سـه تحـول عمده عبارت‌اند از:

الف) جنگ جهانی اول: سال‌های اولیه قرن بیستم، تولد ارتباطـات از راه دور مـدرن (تلگـراف) را نشان می‌دهد و به همراه آن گسترش رمزشناسی و رهگیری، که به‌طور قابل ملاحظـه‌ای در طـول جنـگ رشد کرد. در این جا، نیروی محرکه اصلی فن آوری بود که کشمکش ژئوپلتیک جهانی از آن حمایت کرد.

ب) جنگ جهانی دوم: در اوایل دهه ۱۹٤۰، سازمان‌های اطلاعات محرمانه بر اساس یـک مقیـاس بی سابقه در سرتاسر جهان، با تحول اصلی در استفاده از هیومینت ضداطلاعات، سیگینت و عملیات‌هـای ویژه عمل می‌کردند. دلیل اصلی مسائل جغرافیای سیاسی بود، که یک رشته اختراعات فناورانـه/نظامی کـه در طول جنگ معرفی شده بودند، از آن پشتیبانی می‌کرد. در پایان جنگ، اطلاعات محرمانه و سـازمان‌های امنیتی عضو همیشگی ادارات دولت ملی شد. جنگ سرد، به جز گسترش جهانی نوآوری‌هایی که در طول جنگ جهانی دوم پدید آمده بودند، هیچ چیز واقعاً" جدیدی همراه خودش نیاورد.

ج)"موج سوم":۱۹۸۹-۲۰۰۳: این تحول در یک بازه زمانی ۱٤ ساله، از زمـان سـقوط دیـوار برلین تا حمله آمریکا و انگلیس به عراق رخ داد. این تحول از دگرگونی‌های ژئوپلتیکی و فنی ناشی شد، اما حاصل تغییرات سیاسی – اجتماعی نیز بود. (هدایتی،۱۳۹۳:۱۹۵).

بسترهای تحول در محیط اطلاعاتی و امنیتی

تحول در امور نظامی در اوایل دهه ۱۹۹۰ رخ داد. این مفهوم از دل تغییرات فناوری، سیاسـی، اجتماعی و اقتصادی بیرون آمد که قرار بود به‌طور بنیادین آینده جنـگ را تغییـر دهنـد و یـک نـوع ساختار نظامی و سازمانی کاملاً" جدید بـرای نمـایش مـؤثر نیـرو معرفـی کنـد. هـر چنـد بیش‌تـر متخصصان واقعیت تحول بنیادین در شیوه کار جنگ را پذیرفته‌انـد، امـا تعـداد کمـی یـک تحـول موازی که در دنیای اطلاعات محرمانه رخ دهد را شاهد بوده‌اند، هر چند این حـوزه خـاص امنیـت ملی نیز دستخوش چالش‌ها و تغییرات مشابهی شده است. تحـول در امـور اطلاعـات محرمانـه در

واقع در دهه ۱۹۹۰ و اوایل دهه ۲۰۰۰ رخ داد و تاثیراتش بـه نحـو فزاینـده‌ای مشـهود اسـت. ایـن تحول از ترکیب تغییرات در سیاست‌های بین‌المللـی، فن‌آوری‌هـای اطلاعـاتی و زمینـه سیاسـی – اجتماعی ناشی می‌شود. (هدایتی،۱۳۹۳:۱۷۷).

۱-دگرگونی‌های جغرافیای سیاسی

در اوایل دهه ۱۹۹۰، جامعه اطلاعات محرمانه ضربه سختی از دگرگونی‌های جغرافیایی سیاسی و فروپاشی الگوهای بین‌المللی سابق خورد. جنگ سرد، درگیری که مبتنی بر عملیات‌های مخفیانه اسـت، تقریباً نزدیک به نیم قرن طول کشید. در طول آن دوره، فعالیت‌های سازمان‌های اطلاعاتی در کشورهای عضو سازمان پیمان آتلانتیک شمالی (ناتو) و پیمان ورشو را یک رقابت میان شرق و غرب هدایت می کرد. از دست دادن ناگهانی رقیب، که نفس وجود آن‌ها را تا آن زمان توجیه کرده بود، در ابتدا سازمآن‌ها را گیج کرد و سپس باعث شد آینده خودشان را زیر سؤال ببرند.

۲-تحول فناوری‌های اطلاعات

از اواخر دهه ۱۹۸۰، جهان دستخوش یک تحول گسترده درحوزه فنـاوری بـا نـوآوری‌هـایی در انتقال داده‌ها، الکترونیک و ارتباط از راه دور شد. جهان امروز، تحت تأثیر ترکیب ایـن نـوآوری‌هـا بـه شدت تغییر کرده است. فناوری‌های دیجیتالی که منجر به همگرایی صدا، تصویر و اطلاعات شد، انتقال سریع، پردازش خودکار و افزایش توان محاسباتی و ذخیره سـازی را ممکـن سـاخت. ایـن تحـول در فناوری تأثیر عمده‌ای بر عملکرد اطلاعات محرمانه داشته است.

۳-زمینه‌های اجتماعی- سیاسی جدید

افزایش مطالبات دموکراتیک جدید و ضرورت‌های سیاسی (دولت بهتر، اخلاق، گروه‌های فشار و ...) نیز بر سازمان‌های اطلاعات محرمانه تأثیر گذاشته‌اند. این سه عامل با هم ترکیب شده‌اند تا زمینـه‌ای که این سازمآن‌ها در آن فعالیت می‌کنند، حوزه‌های تمرکز آن‌ها، و نامید[۱] آن‌هـا را تغییـر دهنـد. آن‌هـا تغییرات عمده‌ای را در قوانین حاکم بر فعالیت‌های اطلاعات محرمانه بـه وجـود آورده‌انـد. (نجفـی و پسندیده،۱۳۹۹: ۱۰۹-۱۱۱).

[۱]: Tradecraft تریدکرافت یا نامید: در جامعه اطلاعات محرمانه به شیوه‌های جدید جاسوسی و به طور کلی فعالیت اطلاعات محرمانه اشاره دارد.

پیامدهای تحول فناوری اطلاعات

محدودیت‌های اطلاعات علائم محرمانه

یکی از بزرگ‌ترین تناقضات اطلاعات محرمانه مدرن، اطلاعات محرمانه علائم (سیگینت) است. در کشورهای غربی، اطلاعات محرمانه با ابزارهای فنی در دوران جنگ سرد به‌طور قابل ملاحظه‌ای رشد کرد، عمدتاً" به این دلیل که پژوهش‌های انسانی تنها نتایج محدودی علیه سیستم امنیتی کمونیستی ارائه داد. هشتاد درصد اطلاعات جمع‌آوری‌شده درباره اتحاد جماهیر شوروی از یک منشاء فنی بود. آن ابزارها در حال حاضر کاملاً" محدودشده‌اند. اطلاعات محرمانه فنی، همچنین شاملاطلاعات محرمانه تصویری (ایمینت) نیز می‌شود. و از سوی دیگر این جمع‌آوری‌ها نیز به‌طور فزاینده مؤثر است، اما به چند دلیل نمی‌تواند همه چیز را پاسخ دهد:

۱-رشد ارتباطات از راه دور جهانی

رشد باورنکردنی جوامع مدرن – ارتباطات تلفنی، جی اس ام، اینترنت – چالش اصلی برای سازمان جمع‌آوری اطلاعات علائم است. چهل سال پیش، در سراسر جهان تنها ۵۰۰۰ کامپیوتر استفاده می‌شد. این رایانه‌ها نه به یکدیگر وصل می‌شدند و نه به دستگاه فکس و یا تلفن. امروزه حدود ٤۰۰ میلیون کامپیوتر در سراسر جهان استفاده می‌شود، که همه آن‌ها به هم پیوسته هستند، و همچنین نزدیک به ۲۰ میلیون دستگاه فکس و صدها میلیون تلفن‌های همراه. امروزه، ترافیک شبکه‌های الکترونیکی بیش از دوازده برابر بیش‌تر شده است. البته، توسعه ماهواره‌های جمع‌آوری اطلاعات علائم، همراه با افزایش ظرفیت ابررایانه جدید، پیشرفت‌های قابل ملاحظه‌ای کرده است و ذخیره سازی داده‌ها نیز به سرعت در حال پیشرفت است. با این حال، واقعیت این است که ظرفیت فن آورانه سازمان امنیتی نتوانسته است با رشد ارتباطات از راه دور همگام باشد. حتی ایالات متحده هم نمی‌تواند به‌طور مؤثر صدها میلیون ایمیل، تماس‌های تلفنی و نقل و انتقال پول الکترونیکی که هر روز در سراسر جهان انجام می‌شود را کنترل کند، هر چند تلاش می‌کندچنین کاری را انجام دهد و در میان بی شمار ارتباطاتی که هر روز ایالات متحده نظارت می‌شود، تنها حدود ۱۰ درصد به‌طور جدی به موقع پردازش و تجزیه‌وتحلیل می‌شوند.

۲-توسعه رمزشناسی خصوصی، رمزنگاری به سرعت در حال گسترش است.

رمزگذاری توسط شرکت‌ها و افراد خصوصی هر روز در حال رشد است و چالش عمده‌ای را به سازمان‌های جمع‌آوری اطلاعات علائم تحمیل می‌کند. مبارزه بین رمزشناس‌ها و کسانی که به

دنبال ارتباطات امن هستند، به آرامی به تفوق گروه دوم منجر شده است. البته، شکستن یک کد با قابلیت محاسباتی مناسب همیشه به لحاظ فنی امکان پذیر خواهد بود. اما چنین روندی می‌تواند هفته‌ها به طول انجامد و بیش‌تر تروریست‌ها یا سازمان‌های جنایی تنها برای چند روز، اغلب زمانی که مشغول برنامه‌ریزی عملیات خود هستند، نیاز به حفاظت از مذاکرات محرمانه خود دارند. مهم‌تر از همه، در حال حاضر ابزارهای ارتباطاتی بسیاری در دسترس است که به یک فرد، تروریست و یا جنایتکار امکان دور زدن مسئله رمزگذاری را می‌دهد، به این معنی که بسیاری از آن‌ها می‌توانند، پیام‌های بسیار باارزشی را به سادگی با استفاده از دستگاه‌ها و ابزارهایی که تحت نظارت نیستند، ارسال کنند. برای مثال؛ القاعده از هر دو ابزار مدرن ارتباطی (اینترنت، تلفن‌های همراه رمزگذاری شده وماهواره ای و رادیو) و ماموران مخفی که پیام را منتقل می‌کنند، استفاده می‌کند. با استفاده از چندین تلفن همراه به جای یکی، یک تروریست می‌تواند، استراق سمع سازمان‌های اطلاعاتی را خنثی کند. گاهی اوقات استراق سمع بی فایده است؛ زیرا تروریست‌ها اغلب میان خودشان با استفاده از تماس انسانی مستقیم ارتباط برقرار می‌کنند.

۳-مشکلات ترجمه، چالش دیگر جمع‌آوری اطلاعات علائم

آژانس امنیت ملی گزارش می‌دهد که حدود ٦٥٠٠ زبان در سراسر جهان وجود دارد که مردم به آن‌ها سخن می گویند. پیداکردن تعداد مناسب مترجم برای زبان‌های نادری که سازمان‌های مافیایی یا تروریستی از آن‌ها استفاده می‌کنند، برای سازمان‌های اطلاعاتی بسیار دشوار است. در سال ۲۰۰۰، بخش زبان شناسی دفتر تحقیقات فدرال (اف.بی.آی) ۹۰۰ مترجم و بودجه ۲۱ میلیون دلاری داشت. تا سال ۲۰۰٤، آمار و ارقام به ۱۲۰۰ مترجم و بودجه ۷۰ میلیون دلار رسید. با این حال، در همان سال ۳۰ درصد از ارتباطات رهگیری شده بدون آن که ترجمه شوند، ذخیره شدند. پس از یک دوره سه ساله، به دلیل مشکلات ذخیره سازی داده هار، درصد زیادی از رهگیری ها بدون پردازش حذف شدند.

چالش‌های جدید پردازش داده‌ها

امروزه بیش از گذشته، اطلاعات بیش‌تری در دسترس عموم قرار می‌گیرد. چالش اصلی پیش روی اطلاعات محرمانه مدرن جمع‌آوری اطلاعات نیست، بلکه پردازش داده‌هاست. سه منطقه‌ای که در آن این مسئله به‌طور خاص مهم هستند عبارت‌اند از:

۱-منبع آشکار و رسانه‌های اجتماعی

تحول فناوری اطلاعات انفجاری در منابع اطلاعاتی به وجود آوره است واطلاعات در همه جا و در همه اشکال، از جمله در کتاب‌ها، مجلات، فیلم‌ها، سی دی رم‌ها، اینترنت و رسانه‌های اجتماعی یافت می‌شود. حجم منابع آنلاین با سرعت غیرقابل‌باوری در حال افزایش است. حدود ۱۰۰ میلیون صفحات وب هر روز ایجاد می‌شود، و حجم کلی هر چهار سال دو برابر می‌شود. پایگاه داده‌های تخصصی تجاری که هر روز ایجاد و به روز رسانی می‌شوند، منابع اطلاعاتی جدیدتری به وجود می‌آورند. تصاویر تجاری، منبع جدید در دسترس همگان، به انحصار اطلاعات دولتی از فضا پایان داده است. اخیراً رشد رسانه‌های اجتماعی – توییتر، فیس بوک و سایت‌های مشابه آن‌ها- کانال دسترسی دیگری در اختیار افراد و زندگی خصوصی آن‌ها قرار داده است. فرصت‌های کسب دانش درباره هر موضوعی تغییر کرده است. با توجه به مقدار زیاد داده‌های جمع‌آوری‌شده در هر روز، چالش بزرگی که اطلاعات محرمانه مدرن با آن روبه‌روست تفکیک " گندم از کاه" و " اتصال به نقاط" است.

۲-پروپینت و حفاظت از اطلاعات شخصی

اطلاعات اختصاصی (پروپینت) اصطلاحی است که برای اطلاعات حفاظت شده شخصی موجود در پایگاه‌های دیجیتال که در اختیار هر دوبخش دولتی و یا خصوصی قرار دارد، به کار می‌رود. این حوزه ارتباطات شخصی، جنبش‌ها، مسافرت هوایی، معاملات مالی، وضعیت مهاجرت و سوابق بیمه ملی را مورد توجه قرار می‌دهد. افراد در یک جامعه به شدت پیشرفته به لحاظ فناوری، در حین عبور از فضای مجازی از زندگی خودشان رد به جا می‌گذارند. پروپینت برای مبارزه با تروریسم و یا جاسوسی بسیار مفید است، بسیار بیش‌تر از اوسینت (اطلاعات محرمانه منابع آشکار). این پایگاه داده‌ها از نظر قانونی، بسته به قوانین قابل اجرای حفاظت از اطلاعات شخصی، در دسترس سازمان‌های اطلاعاتی و امنیتی هستند یا شاید نیستند. هر کشور رویکرد و قانون متفاوتی برای حفاظت داده‌ها دارد، اما در اغلب موارد بهای آن پایان یافتن حریم خصوصی افراد است.

از بیست سال پیش تاکنون، مقدار داده‌ها و محصولاتی که باید پردازش شوند با شرعت زیادی افزایش یافته است. کار سازمان‌های اطلاعاتی تغییر کرده است، چراکه آن‌ها حوزه‌های فعالیتشان را گسترس داده‌اند. آن‌ها باید مهارت‌های جدید را در جهات جدید مانند فناوری، امور مالی، اقتصاد، تحقیقات بازاریابی، تغییرات آب و هوا و جرم و جنایت بین‌المللی گسترش دهند. تحول اطلاعات ابزارهای جدید زیادی به وجود آورده است: داده کاوی و نرم افزار تجزیه‌وتحلیل خودکار و افزایش

ظرفیت ذخیره سازی، افزایش کامپیوتر و داده‌ها. اما دشمنان و یا اخلال گران نیـز از ایـن ابزارهـا بـرای اهداف جنایی استفاده می‌کنند. این به آن‌ها قدرت بی بدیل برای فعالیت‌های مخفیانه می‌بخشـد؛ حتـی سازمان‌های کوچک می‌توانند از مزایای فناوری کم هزینه برای گسترش سیستم‌هـای اطلاعـاتی بسـیار کارآمد بهره ببرند.

خصوصی سازی و تنوع گردانندگان و تولید کنندگان اطلاعات محرمانه

تحول اطلاعات همچنین منجر به توسعه شرکت‌های خصوصی اطلاعات محرمانه، ایجاد شرکای جدید و همچنین رقبای جدید برای سازمان‌های دولتی شده است.

۱-شرکای جدید: شرکت‌ها مشتریان جدید اطلاعات محرمانه هستند.

در طول دهه گذشته، رقابت‌های اقتصادی بسیار شدیدتر شده است. همـین مسـئله باعـث شـده است بسیاری از شرکت‌ها به‌منظور توسعه قابلیت‌های اطلاعات محرمانـه تجـاری، خودشـان نیازهـای اطلاعاتی‌شان را برآورده کنند و از خودشان در برابر فعالیت‌های ایجاد کننده بی ثبـاتی محافظـت کننـد. مشاوران ارائه دهندگان جدید اطلاعات محرمانه هستند. بسـیاری از مشـاوران بیش‌تـر اعضـای سـابق سازمان‌های امنیت ملی – از این بازار جدی برای گسترش تجارت خودشان نهایت بهره را برده‌انـد. بـه آن‌ها مأموریت‌هایی داده می‌شود که قبلاً" بخشی از وظایف سازمان‌های دولتی بود. برخی از آن‌هـا نیـز مأموریت‌های اطلاعات محرمانه، آموزش و یا مأموریت‌های امنیتی را به نمایندگی از سازمان‌های دولتی انجام می‌دهند. در سال ۲۰۱۰، مدیر تازه منصوب شده اطلاعات ملی آمریکا متوجه شد که ۷۰ درصـد بودجه اطلاعات محرمانه به پیمانکاران خصوصی اختصاص داده شده بود و ۵۰ درصد کارمنـدانی کـه برای سازمان اطلاعات محرمانه دفاعی کار می‌کنند، پیمانکاران خصوصی بودند. بخش صنعت نیز طیف گسترده‌ای از محصولات اطلاعات محرمانه را از پایگاه داده‌ها گرفته تا نرم افزار، ارائه داده است.

۲-رقبای جدید

خصوصی سازی اطلاعات محرمانه موقعیت سنتی سازمان‌های دولتی، که برای مدت طولانی تنها منابع سیاست‌گذاران بود را به چالش می‌کشاند. برای اولین بار در تاریخشان، این سازمان‌های دولتی در رقابت با عوامل جدید بخش خصوصی، که اغلب قادر به ارائه اطلاعات بـا کیفیـت بـالا، و گاهـا" بـا سرعت و دقت بیش‌تر از سازمان آن‌ها بودند، قرار گرفتند. درنتیجه، سازمان‌های اطلاعات محرمانه ملی باید نوعی مقایسه با فعالان حوزه خصوصی را می‌پذیرفتند. (نجفی و پسندیده،۱۳۹۹: ۱۱۸-۱۲۳).

چالش‌های اطلاعات آشکار

دلیل و برهان آوردن برای اجتناب از اطلاعات آشکار تا حدی شبیه این است که بگوییم چون هوا پر از مواد مواد سرطان زا و زیان بار است، بهتر است نفس نکشیم. اطلاعات آشکار، عامل حیاتی کار اطلاعاتی است. اعداد و ارقام متفاوتند اما به نظر می‌رسد اکثر آنها بر این توافق دارند که اطلاعات آشکار ۷۰ إلی ۸۰ درصد پایگاه داده‌های اطلاعاتی ایالات متحده را تشکیل می‌دهد. با پایان جنگ سرد و باز شدن بسیاری از بخش‌های جهان که جامعه‌های بسته در نظر گرفته می‌شدند، احتمال دارد که حتی همین تخمین هم بسیار پایین باشد. به استثنای کره شمالی، عراق، و شاید بلاروس، امروزه تعداد محدودی از جوامع به‌اندازه‌ای دقیق کنترل می‌شوند که کسب آگاهی درباره آنها از طریق اطلاعات آشکار دشوار باشد. و حتی در این جوامع بسته هم موانع در حال برداشته شدن است.

با این همه، احتمال دارد اطلاعات آشکار در ردیابی بازیگران غیردولتی مانند تروریست‌ها، چهره‌های مجرم بین‌المللی، و یا قاچاقچیان مواد مخدر چندان سودمند نباشد. با این وجود، نوارهای ساخته شده به دست بن لادن نشان می‌دهند که در برخی مواقع بازیگران غیر دولتی هم ممکن است اقدام به تولید اطلاعات آشکار کنند. بعضی گروههای تروریست تا جایی پیش رفته‌اند که برای خود وب سایت ساخته‌اند. شاید این کار در راستای تبلیغات شخصی آنها باشد ولی اغلب ارزش همان نوع از مطالعه‌ای را دارد که تحلیل گران اطلاعاتی در زمان جنگ سرد بر روی منابعی مانند رادیو مسکو و خبرگزاری چین جدید انجام می‌دادند.

۱-منطق متعارف

عقیده عمومی این است که بزرگ‌ترین مشکل، حجم زیاد اطلاعات آشکار است که بر توانایی تحلیل گران برای دسته بندی آن تأثیر می‌گذارد. این فشار، اگرچه جدید نیست، با، داده‌های منابع آشکار در سال‌های اخیر تشدید شده است. در واقع، این موضوع همواره یک مشکل اساسی کار اطلاعاتی و نه فقط در اطلاعات اشکار بوده است سال‌هاست که آژانس ملی اطلاعات آشکارا از رمز گشایی و تفسیر برخی اطلاعات به‌دست‌آمده از شنود پیام‌ها عاجز بوده است.

۲-پروژه‌های جدید

در راستای رسیدگی به اشباع اطلاعاتی، آژانس مرکزی اطلاعات (سیا) جهت توسعه تکنیک‌هایی برای دسته بندی، نظم دهی و انتقال اطلاعات خام به بخش خصوصی روی آورده تا تحلیل گران از این بابت تحت فشار قرار نگیرند. سازمان سیا به دنبال سرمایه گذاری در مؤسساتی بوده که بتوانند از عهده

این کار برآیند و بدین منظور، سازمانی را با نام این کیوتل[1] تأسیس نموده و از آن حمایت مالی می‌کند، که یک «شرکت سرمایه گذاری خصوصی و غیر انتفاعی است». بسیاری از اقداماتی که مورد حمایت مالی قرارگرفته به‌منظور «داده کاوی» و «مدیریت دانش» طراحی‌شده تا بتواند الگوها و یا ناهمسانی‌هایی را در جریان‌های گسترده داده‌های خام کشف کند. تحلیل گران اطلاعاتی واقعاً "معتادان اطلاعات" هستند. آن‌ها هیچ وقت باور ندارند که اطلاعاتی که در دست دارند، بیش از حد لازم زیاد باشد. آن‌ها همیشه امیدوارند که یک قطعه کلیدی از پازلی که در حال حل کردن آن هستند، موجود است؛ فقط اگر بتوانند آن را پیدا کنند. بدین ترتیب، هر سیستمی که حجم اطلاعاتی را که در دسترس تحلیل گر قرار می‌گیرد محدود کند، احتمال دارد به نحوی قطعه‌ای کلیدی از اطلاعات را پنهان کند. تحلیل گران همیشه مایل بوده‌اند انبوهی از اطلاعات را غربال کنند تا به آن قطعات کلیدی که به دنبالش هستند، دست یابند. درنتیجه، تکثر اطلاعات آشکار، بیش‌تر یک موهبت است تا بلا. آنچه که تحلیل گران بدان نیازمنداند، پیدا کردن روشی سریع برای سازمان‌دهی اطلاعات و جستجوی سریع در میان داده‌هاست. هدف پروژه‌های جدید، رفع این مشکل است.

۳-مسائل مرتبط با قابلیت اعتماد

چالش دیگر اطلاعات آشکار، غیر قابل اعتماد بودن آن می‌باشد. این موضوع همیشه صحت داشته اما در طول زمان، همان طور که تقریباً درباره هر نوع دیگری از منابع اطلاعاتی چنین بوده است، تحلیل گران یاد می‌گیرند که به چه منابعی اعتماد کنند و چه منابعی به احتمال قوی نادرست، تحریف شده، جانبدارانه، تبلیغاتی و یا فریب خبری هستند.

٤-اطلاعات آشکار و فریب خبری

مطالعه فریب‌های خبری در اطلاعات آشکار نشان می‌دهد که رسانه‌های عمومی اغلب می‌توانند به‌منظور بدنام کردن دشمن و یا انتشار اخبار غلط به‌صورت پنهان شده در لایه‌ای از حقیقت به کار روند. در طول جنگ سرد، کشورهای عضو پیمان ورشو از سازمان امنیت چکسلواکی به‌منظور انتشار فریب خبری استفاده می‌کردند. تحلیل گران اطلاعاتی می‌توانند چنین فریب‌های خبری را برای ردگیری این که چگونه این اطلاعات منتشر شده و با داستآن‌های رسانه‌ای در آمیخته می‌شود، سودمند یابند. استفاده از رسانه‌ها برای فریب خبری و یا انتشار اطلاعات گمراه کننده، می‌تواند شمشیری دولبه باشد. در جنگ جهانی دوم، متفقین با موفقیت توانستند اطلاعات آلمان را قانع کنند که عملیات فرود نورماندی تنها

[1] IN-Q-TEL

مقدمه‌ای بر حمله اصلی – که هرگز انجام نشد در ناحیه کالـه می‌باشـد. همچنـین «جنـرال اچ. نـورمن شوارتسکف» تکنیک‌های مشابهی را برای فریب دادن صدام حسین به کار برد تا او تصور کند نیروهای مأمور به آزاد سازی کویت، نقشه حمله از دریا را در سر دارند نه یک حمله زمینی را.

۵–فن مخفی نویسی

امروزه آشکارا از ایترنت برای تکنیک قدیمی مخفی نویسـی اسـتفاده می‌شـود. بنـا بـه گزارش‌هـا، تروریست‌ها، قادر به پنهان سازی پیام‌های مخفی بر روی ایترنت جهت ارتباط بـا پیـروان خـود بوده‌انـد. کشف این پیام‌ها نیازمند مهارت تکنیکی است که ممکن است تعریف اطلاعات اشکار را گسترده‌تر سازد.

٦–میکرودات

در قرن نوزدهم، تکنیک‌های اولیه عکاسی به‌اندازه‌ای پیچیده شدند که میکرودات به وجود آمد، که در آن اندازه یک پیام به قدری کوچک می‌شود که می‌توان آن را در یک صفحه مطالب چاپ شده پنهان کرد. تا قرن بیستم، تکنیک‌های عکاسی به‌اندازه‌ای پیشرفته شده بود که میکرودات بخشـی از مجموعـه استاندارد شگردهای جاسوسی شد. اگر منبع گردان جاسوس بداند به کجا باید نگـاه کنـد، میکـرودات می‌تواند به آسانی از صفحه برداشته شده و به‌اندازهای بزرگ شود که پیام قابل مشاهده باشد. در عصـر کنونی با توجه به پیشرفت‌های فناوری و تکنولوژیک، بهره برداری از این تکنیک به مراتب پیچیـده‌تر و کشفان دشوارتر گردیده است.

۷–زبآن‌های ناشناخته و خدمات اطلاعاتی رسانه‌های خارجی

یک مساله مرتبط با مشکل پیام‌های مخفی، ناکامی مستمر اطلاعات ایالات متحده امریکا از تفسیر و درک داده‌های اطلاعاتی موجود در زبآن‌های ناشناخته و گویش‌هـای قبیلـه‌ای اسـت. پـس از یـازده سپتامبر ۲۰۰۱، فراخوانی برای صحبت کنندگان به زبآن‌های دری و پشتو منتشر شد، اما دیگر دیر شـده بود. سرویس‌های اطلاعاتی از دو مشکل مجزا رنج می‌برند. مشکل اول، تقلیل بودجه و کاهش پرسـنل در سازمانی است که خدماتی در رابطه با مساله ای عمومی که ترجمه‌هایی از رسانه‌ها را در اختیار مـی گذاشت، بود و مشکل دوم، ناتوانی آن‌ها در ترویج مطالعات زبان شناسی و فرهنگی است.

۸–اطلاعات آشکار و مصرف کنندگان

اطلاعات آشکار، علی رغم تمامی کاربردهایش، مورد تقاضای زیادی از جانب مصرف کننـدگان نیست. تصمیم گیران سیاسی از جامعه اطلاعاتی انتظار دارند اطلاعات و تحلیل‌هـایی را در اختیارشـان قرار دهد که در مطالعه و مشاهده خودشان از رسانه‌ها موجود نباشد. در واقع مطالعات نشان می‌دهد که

مصرف کنندگان اطلاعات گاهی برای رسانه‌ها، بیشتر از محصولات اطلاعاتی که دریافت می‌کنند، ارزش قائلند. مصرف کنندگان، خواهان اطلاعات به‌دست‌آمده از طریق مأمورین و منابع مخفی هستند – اطلاعاتی که خودشان نمی‌توانند در نیویورک تایمز بخوانند.

۹–در دسترس گذاشتن اطلاعات آشکار برای دشمنان

یک جنبه منفی ناخوشایند اطلاعات آشکار این است که تا چه مقدار از آن باید در دسترس دشمنان باشد. در سراسر جنگ سرد، زمانی که ایالات متحده متحمل میلیونها هزینه می‌شد تا «دشمن» خود، شوروی را تحت نظر بگیرد، اتحاد جماهیر شوروی هزینه نسبتاً کمی برای کنترل ایالات متحده صرف می‌کرد. در حالی که آمریکا مشغول ساخت هواپیماهای جاسوسی یو–۲ و اس آر–۷۱ و ماهواره‌های پیچیده تقریباً زمان واقعی (بلافاصله) برای ردیابی موشک‌ها، زیردریایی‌ها و هواپیماهای شوروی بود، مسکو می‌توانست مأمورین خود را به تاسیسات نظامی بفرستد تا در بازدیدهای عمومی، نمایش‌های هوایی، و بازدید از کشتی‌ها شرکت کنند.

اخیراً حکومت ایالات متحده متوجه شد که آن دسته از راهنماهای تسلیحات بیولوژیک و شیمیایی‌اش که متعلق به دهه ۱۹۵۰ بوده، از محرمانگی خارج شده و در دسترس عموم قرارگرفته است. برخی مقامات فکر کردند که این اطلاعات باید جمع‌آوری‌شده و مجدداً محرمانه شود. چنین کاری بدون شک عملی بیهوده است. به محض آنکه اطلاعات از محرمانگی خارج شده و در اختیار عموم قرار می‌گیرد، باید بنا را بر این گذاشت که همه به آن اطلاعاتی که در گذشته مخفی بوده دسترسی یافته‌اند و خسارت دیگر وارد " است. برخی مقامات حکومتی پیشنهاد کرده‌اند که اطلاعاتی که در حال حاضر غیر محرمانه شده اما هنوز برای عموم منتشر نشده، مورد بازبینی قرار بگیرد. اگر انتشار آنها خطری را به دنبال دارد، این اطلاعات می‌تواند دوباره محرمانه شود. (هدایتی،۱۳۹۳: ۹۳–۱۰۵).

چالش‌های امنیت سایبری

فضای سایبری (و لایه‌های فیزیکی، منطقی و اجتماعی تشکیل دهنده آن) چالش‌ها و فرصت‌هایی جدی را برای سازمان‌های اطلاعاتی به وجود می‌آورند. به مدد پیشرفت‌های سریع در تکنولوژی، قابلیت‌هایی که زمانی تنها در اختیار دولت‌ها قرار داشتند امروزه به‌صورت گسترده در اختیار افراد قرارگرفته‌اند. علاوه بر این، ناشناخته ماندن نسبی در فضای سایبری به معنای آن است که این قابلیت‌ها را می‌توان با محدودیت‌های اندکی به کار گرفت. این موضوع منجر به ایجاد چالش‌های جدیدی در این حوزه گردیده است.

۱–چالش‌های سیاسی

ابعاد سیاسی امنیت سایبری و اطلاعات در حال گسترش است و این مسائل در ابعاد مختلف خود به وسیله پیشرفت‌های فنی (یعنی پردازشگرهای سریع‌تر، قابلیت ذخیره سازی بیشتر، سنسورهای بسیار پیشرفته، الگوریتم‌های پردازش داده پیشرفته، کدگذاری‌های قوی) هدایت و کنترل می‌شوند، که چشم اندازهای جدیدی را برای جمع‌آوری و تحلیل ارائه می‌دهند. این پیشرفت‌ها مورد استقبال برخی دولتها قرارگرفته و برخی دیگر با دیده تردید و نگرانی با آنها رفتار کرده‌اند، و این موضوع تا حدودی وابسته به گستره منافع محافظت شده‌ای دارد که با چالش مواجه شده‌اند. فضای سایبری، خطرات سیاسی و فیزیکی جمع‌آوری اطلاعات را کاهش داده و آن را به یک فعالیت جذاب و کم خطر با بازدهی زیاد تبدیل کرده است. با این حال هم چنان چالش‌های سیاسی قابل توجهی وجود دارد. بزرگ‌ترین این چالش‌ها، درک غلط از ماهیت فضای سایبری می‌باشد، به‌طور خاص درک قدرتی که این فضا برای اقدامات غیر متمرکز در سطوح فردی و گروههای کوچک به وجود می‌آورد مهم‌ترین موضوع است.

۲–از بین رفتن تمرکز قدرت

فضای سایبری ارائه دهنده فرصت‌هایی قابل توجه برای تمرکز زدایی از قدرت است که در بر گیرنده اقداماتی مستقل و با جمعی است. احتمالات و حالت‌های عملی این تمرکززدایی به‌منظور ایجاد نوآوری‌های غیر مجاز و توسعه و به کارگیری تکنولوژیکی‌های جدیدی که دستگاه‌های تأسیس شده و منافع محفوظ شده را مختل می‌نمایند، گسترده هستند. سازمان‌های اطلاعاتی بایستی خود را با این محیط و استفاده‌های خلاقانه عمومی از تکنولوژی وفق دهند. قابلیت‌های قدرتمندی هم چون تصویربرداری ماهواره‌ای با کیفیت بالا و موقعیت یابی ماهواره‌ای، امروزه به‌صورت گسترده و به کمک دستگاه‌های استفاده کننده اینترنت یا داده در دسترس هر فردی است. پیشرفت‌ها در کوچک سازی چنین دستگاه‌هایی این امکان را فراهم نموده تا حمل و نقل و پنهان سازی آن‌ها به‌راحتی انجام شود. بسیاری از این پیشرفت‌ها در ابتدا از بخش‌های خصوصی و در پاسخ به نیازهای تجاری ظهور پیدا کرده‌اند. در دسترس بودن این سطح از پیچیدگی‌های تکنولوژیکی به‌صورت سنتی برای محافظت از دولت‌ها بوده است و نه افراد، و تمرکز زدایی از این قدرت به وسیله بسیاری از دولت‌ها به‌عنوان یک چالش اساسی مد نظر است.

۳–عدم قطعیت

یکی از وظایف یک سازمان اطلاعاتی را می‌توان در قالب "غلبه بر عدم قطعیت" در نظر

گرفت. به‌عنوان بخشی از این موضوع، ضروری است تا فهم صحیحی از نیروهای فعال (متغیرهـای کلیدی و گردانندگان سیستم و هم چنین چشم انـدازی از دشـمنان خـود) در هـر موقعیـت وجـود داشته باشد. این مسئله تفاوت بین فهـم اسـتراتژیک و فرمانـدهی تـاکتیکی بـرای یـک موضـوع را مشخص می‌نماید. به بیان دیگر، هر چیزی که اجازه می‌دهد تا نگاه ما به دشمن بهبـود یابـد (بـرای مثال، جاسوسی، به اشتراک گذاشتن اطلاعات با متحدان، پردازش داده‌های دقیق) می‌تواند به کسـب یا حفظ یک حد کیفی کمک نماید.

امنیت شبکه و داده یکی از نگرانی‌های همیشگی در ارتباط با امنیت سایبری و ضد جاسوسی بوده است. در هنگام دفاع در مقابل نفوذهای پیشرفته، تشخیص دادن این که متجاوز در حال جاسوسی و یا شناسایی‌های خصمانه است بسیار سخت است. هر دو این موارد جزو نگرانی‌های هستند، با این حـال مورد دوم به مراتب شدیدتر است و می‌تواند نشانه‌ای از آماده سازی میدان نبرد برای حمله باشـد. ایـن ابهام زمانی شدیدتر می‌شود که هم چون بسیاری موارد دیگر، کشف تجاوز بسیار دیر و زمانی اتفاق می افتد که اطلاعات دزدیده شده و کامپیوترهای حاوی داده‌ها پاکسازی شده‌اند. در چنین شرایطی، انجـام تحلیل منطقی احتمالاً غیرممکن بوده و بـرآورد خسـارت مـبهم و تقریبـی اسـت. بخـش عمـده‌ای از زیرساخت‌های حیاتی در مالکیت بخش خصوصی بوده و توسط این بخش فعال هستند. علاوه بر این آنها منبعی غنی از دارایی‌های فکری هستند که همین موضوع آن‌ها را بـه اهـداف اطلاعـاتی عمـده‌ای تبدیل می‌کند. تعداد اندکی از این شرکت‌های حساس می‌توانند به‌صورت مسـتقل و موفقیـت آمیـز در مقابل تلاش‌های اطلاعاتی یک دولت متخاصم با منابع فراوان مقاومت نمایند. با این وجـود، موانـع بـه اشتراک گذاری اخبار (مثلاً محرک‌های واگرا) از اقدام دفاعی هماهنگ بخش‌های خصوصی دولتی جلو گیری می‌نمایند و این موضوع با توجه به تهدیدات کمی و کیفی فضای سایبری سـبب افـزایش عـدم اطمینان کل می‌شود. از منظر عمومی یک نقص خاص در ارتباط با اخبار تهدید آمیز وجود دارد که حتی مانع از محاسبه یک معادله ریسک اساسی (ریسک = تهدید * آسیب پذیری * اثرات) می‌شود.

٤-گشایش

امروزه، I CT مدرن به مشتریان اطلاعاتی خود اجازه می‌دهد تا تحلیل داده‌های خـام خـود را در زمانی واقعی و سریع انجام دهند. علاوه بر این به آنها اجازه می‌دهد تا به منابع بی‌شماری دسترسی پیدا کنند که بسیاری از آنها مربوط به دولت نیست. (مثلاً خروجی رسانه‌ها، وبلاگ‌ها، رسانه‌های اجتماعی). سازمان‌های اطلاعاتی با توسعه بخش‌هایی که منحصراً بـر روی اطلاعـات آشـکار (OSI NT) تمرکـز

نموده‌اند (مثلاً مرکز منابع آشکار CI A) به این چالش پاسخ داده‌اند. برخی اوقات آنها حجم عظیمی از داده‌ها را مورد بررسی دقیق قرار اند تا سرنخ کوچکی به دست آورند، با این حال به‌صورت فزاینده‌ای به الگوهای جدید برای طبقه بندی انواع مختلف داده‌ها (مثلاً ایمیل، پیام کوتاه، مختصات مکانی، رسیدهای بهداشتی، مالیاتی، قانونی و جنایی) دست یافته‌اند. این موضوع به‌صورتی بدیهی یک وضعیت مطلوب در نظر گرفته می‌شود ولی هنوز رشد کمی برابر با بهبود کیفی نبوده است. منابع اطلاعاتی بسیاری وجود دارد که در رقابت با یکدیگر سعی دارند تا توجه تحلیل گران و مشتریان اطلاعاتی را به خود جلب نمایند، با این حال نکته مهم محدودیت زمانی است.

۵–چالش‌های انسانی و اجتماعی

فضای سایبری دربرگیرنده چالش‌هایی با ابعاد انسانی و اجتماعی برای اطلاعات است. با وجود آن که جمع‌آوری اطلاعات در فضای سایبری را می‌توان افزایش داد و این امر می‌تواند به‌عنوان مکملی برای اطلاعات حاصل از منابع انسانی باشد ولی نمی‌تواند جایگزین آن شود. انسان بخش ضروری فازهای پردازش و تحلیل است. کامپیوترها در پردازش حجم انبوهی از داده‌ها بسیار کارآمد هستند. با این حال در توانایی تأمین تحلیل‌های چند وجهی با شرایط خاص که حضور انسان در آنها ضروری است محدودیت دارند. در طیف داده > اخبار > دانش > هوش، کامپیوترها در کنترل دو دسته اول غالب هستند در حالی که حضور انسان برای دو دسته آخر ضروری است. عنصر انسانی هر دو مؤلفه ضعیف‌ترین ارتباط و قوی‌ترین حضور را به‌صورت همزمان در فضای سایبری دارا است. پتانسیل مهندسی اجتماعی (یعنی اجرا یا تحریک مردم به ایجاد یک ضعف امنیتی) یکی از بارزترین ضعف‌های ساختاری در هر سازمانی است. با این حال تنها انسان می‌تواند داده را تبدیل به دانش کند یا اشتباهات موجود در نتایج تولید شده توسط یک کامپیوتر را مشخص نماید. چالش موجود، دانستن زمان اضافی بودن انسان در حلقه و زمان ضروری بودن وی در آن است.

٦–چالش‌های تکنولوژیک

پیشرفت‌های تکنولوژیکی همان گونه که فرصت‌های جدیدی را برای سازمان‌های اطلاعاتی به وجود آورده‌اند، چالش‌های جدیدی را نیز برای آنها به وجود آورده‌اند. با این حال از آن جا که فضای مشکلات به لحاظ تاریخی آشنا و نسبتاً شناخته شده است، به‌صورت قابل ملاحظه‌ای ابهامات در این حوزه اندک است. نسبت به دیگر سازمان‌های دولتی، سازمان‌های اطلاعاتی تمایل دارند تا خود را سریعتر با تکنولوژی‌های جدید وفق دهند. در چرخه تأمین و تقاضای جمع‌آوری اطلاعات، بخش

تأمین کننده به‌طور پیوسته از منابع جدید داده و روش‌های جمع‌آوری استقبال می‌نماید. این فرصت‌ها به خودی خود ارائه کننده چالش‌های جدیدی هستند و امکان دسترسی به سیلی از داده‌ها را به وجود می‌آورند که سازمان در حال جمع‌آوری آنها است. احتمالاتی که ورای بزرگ‌ترین آرزوها و خواسته‌های سازمان‌های اطلاعاتی در پس فضای سایبری وجود دارد و دستاوردهای حال و آینده، خود به‌اندازه کافی دارای منافع قابل توجه برای سرمایه گذاری هنگفت در منابع انسانی، فرآیندها و تکنولوژی مربوط به این حوزه هستند. ضداطلاعات و دفاع شبکه‌ای از چالش‌های ثابت سازمان‌های اطلاعاتی هستند، در حالی که در همین زمان اطلاعاتی تلاش می‌نمایند تا به شبکه‌های دولت‌های دیگر نفوذ کنند. طراحی و سازمان‌دهی شبکه‌های امنیتی کاری حساس و پر زحمت است که ایجاد یک تغییر در یکی از بخش‌های آن منجر به مجموعه‌ای از تغییرات متناظر در شبکه می‌شود.

۷-تعیین هویت

تحلیل گران تنها افرادی نیستند که با فضای سایبری سر و کار دارند. گسترش تکنولوژی و افزایش شبکه‌های ارتباطی فرصت‌های جدیدی را برای وجوه بسیاری از اطلاعات به وجود آورده است، با این حال این موضوع موانعی را در حوزه‌های دیگر به وجود آورده است. یکی از چالش‌های اساسی، گسترش کنترل‌های پیچده (اغلب بیومتریک) در گذرگاه‌های مرزی بوده است. ایجاد هویتهای چندگانه برای پرسنل اطلاعاتی که به‌طور مرتب به یک کشور مشابه مسافرت می‌کنند بسیار سخت‌تر شده است. این مشکل تنها سبب افزایش کنترل‌های بیومتریک از قبیل اسکن عنبیه چشم شده که صورت گسترده‌ای در سرتاسر جهان مورد استفاده قرار می‌گیرد. این روش با پیشرفت‌ها در تکنولوژی تشخیص چهره همراه شده و بر افسران اطلاعاتی و پلیس مخفی، هم چنین مخالفان سیاسی یا هر کسی که آرزوی ناشناخته و مستقل بودن را دارد تأثیر گذاشته است. گسترش تکنولوژی پیشرفته، وجوه سنتی فعالیت‌های جمع‌آوری از طریق منابع انسانی را بسیار سخت کرده و مسئله تعیت هویت تأثیرات آشکاری بر بسیاری از حوزه‌ها گذاشته است. ایجاد اطلاعات دیجیتال غیر واقعی قابل باور در فضای سایبری، برای کمک به ایجاد یک پوشش یا وجوه دیگری از یک هویت جعلی یا جانبی، سخت‌تر شده است. (معاونت پژوهش و تولید علم، ۱۳۹۵: ۱۸-۲۸).

چالش‌های فراروی چرخه اطلاعات(جمع‌آوری، هدایت، تحلیل، توزیع)

اکنون کاملاً مشخص شده است که چرخه اطلاعات با توجه به تحولات فناوری و اطلاعاتی، دیگر کارایی گذشته را ندارد و کهنه شده است. تغییر در ماهیت تهدیدها و اهداف و همچنین انقلاب

اطلاعاتی همگی باعث شده‌اند که مدل کلاسیک چرخه اطلاعات دست کم نیازمند یک بازنگری اساسی باشد. برخی از چالش‌های فراروی چرخه اطلاعات در عصر اطلاعات عبارت‌اند از:

۱- جامعه باز

توان طرف‌های خارجی برای جمع‌آوری مقادیر عظیمی از اطلاعات، آن هم اغلب به شکل قانونی، لازمه طبیعی سیستم حکومت داری باز و مردم سالاری است که به شفافیت، آزادی و همکاری بها می‌دهد. آسیب پذیری های ذاتی چنین سیستمی در پرونده تازه مأموران روسی که پیش از اخراج از آمریکا، سال‌ها در این کشور آزادانه زندگی و کار می‌کردند، آشکار است. یکی از مدیران سابق ضداطلاعاتی می‌گوید که تعداد انبوه شرکت‌های در مالکیت خارجی، تجارت فرامرزی و تبادل دانشجویان، گردشگران، دانشگاهی‌ها و شخصیت‌های دنیای کسب و کار جامعه‌ای «سفارشی ساز» برای فعالیت‌های پنهانی گردآوری اطلاعات خلق می‌کند. حرکت مستمر به‌سوی گشودگی بیش‌تر، شبکه سازی اجتماعی و مبادله آزاد اطلاعات فقط کار موجودیت‌های خارجی را برای برنامه‌ریزی، هدف گیری و دستیابی به اطلاعات ارزشمند آسان‌تر می‌کنند. با ورود نسل‌های آمریکایی پرورش یافته در این عصر گشودگی که هیچ نوع اطلاعات شخصی یا حرفه‌ای را حساس یا حتی انحصاری نمی‌دانند به بازار کار، چالشی بی مانند برای مدیران و افسران اطلاعاتی به وجود می‌آید.

۲-تغییرات سریع فناوری

پیشرفت‌های سریع فناوری در ذخیره سازی و پردازش داده‌ها، شبکه سازی و ارتباطات کنترل و مهار اطلاعات را سخت‌تر و سخت‌تر کرده‌اند. دولت، شرکت‌ها و صنایع برای پردازش، انبارش، تحلیل و انتقال اطلاعات حساس، به شکلی فزاینده، به این فناوری‌های تازه متکی می‌شوند. ارتباطات با مشتریان و شرکا اهمیتی همیشگی دارد. توان جست و جو، دستیابی، بارگذاری و انتقال سریع حجم عظیمی از اطلاعات برای هر کسی که درصدد جاسوسی باشد، مزیتی قطعی است. به لطف توان دستیابی سریع به انبوهی از داده‌ها در فقط یک حمله موفق، پتانسیل آسیب زدن به شکلی چشم گیر افزایش یافته‌اند اکنون فناوری به دشمنان امکان می‌دهد که بسیاری از حمله‌ها را از راه دور ترتیب دهند. عمل جاسوسی را که زمانی مستلزم دسترسی فیزیکی بود، حالا می‌توان ان فاصله‌ای دور اجرا کرد که باعث ناشناس ماندن و مصونیت گردآوری کنندگان اطلاعات می‌شود.

۳-محیط رقابتی کسب و کار

رقابت شدید میان شرکت‌ها و صنایع، در کنار نیاز دولت‌ها به حفظ برتری خود در دستگاه‌های

نظامی، بازار گرمی برای اطلاعات صنعتی، فناوری‌های پیشرفته و اسرار تجاری به وجود آورده است. از بسیاری جهات، رقابت تجاری و انگیزه کسب سود، به جای ایـدئولوژی، عوامـل انگیزشـی جاسوسـی شده‌اند. رقابت اقتصادی، به شکلی فزاینده، دولت‌ها و شرکت‌های خارجی را به بازار خریـد اطلاعـات حساس مربوط به فناوری می‌کشاند. این روند باعث انتقال تولید، تحقیق و توسعه به مکآن‌هایی مخاطره آمیز تر می‌شود؛ مکآن‌هایی که محیط امنیتی و قانونی در برابر جاسوسی و سرقت اسرار تجاری کمتر از شرکت‌ها حفاظت می‌کند. (ولز و دیگران،۱۳۹۳: ۵۷–۵۸).

٤– جهانی شدن نیروی کار

جهانی شدن بخش‌های تجاری، شرکت‌ها و دانشگاه‌ها، به خصوص در حوزه‌های علمی و فنـی، فرصت‌های مناسبی را برای سرویس‌های اطلاعاتی خارجی جهت جـذب و اسـتفاده از شهروندانشـان به‌عنوان عوامل غیرستی جمع‌آوری اطلاعات فراهم مـی‌آورد. بـه گـزارش اف بـی آی، سـرویس‌های اطلاعات خارجی در شناسایی و جذب دانشجویان، گردشگران و مهـاجران حاضـر در خـاک ایـالات متحده برای دسترسی به اطلاعات ارزشمند بیش از گذشته فعال شـده‌اند. (معاونـت پـژوهش و تولیـد علم،۱۳۹۳: ۲۳۰)

۵–چالش پردازش اطلاعات

عصر اطلاعات، جریان آزاد اطلاعات و دسترسی به حجم انبوهی از اطلاعات امری عادی به نظر می‌رسد. اولین تأثیر این ویژگی عصر اطلاعـات بـر سـازمانهای اطلاعـاتی ایـن اسـت کـه از اهمیـت جمع‌آوری اطلاعات کاسته می‌شود، زیرا بخش اعظم اطلاعات مورد نیاز در قالب اخبار آشکار موجود است. بنابراین آنچه اهمیت بیشتری می‌یابد پردازش انبوهی از اطلاعات است که در اختیار سـازمانهای اطلاعاتی قرارگرفته است. پردازش چنین حجمی از اطلاعات چالشی عملی و واقعی است. در حقیقت درصورتی‌که همراستا با افزایش حجم اطلاعات، توان تحلیل رشد نکند، استانداردهای تائیـد اطلاعـات درست از غلط افت خواهد کرد و ایـن بـدین معنـی اسـت کـه اطلاعـات غلـط وارد خروجـی‌هـای سازمان‌های اطلاعاتی می‌شود و مبنای تصمیم گیری سیاستمداران قرار می‌گیرد. (دیو سالار،۹۲:۱۳۹٤)

۲–چالش تحلیل اطلاعات

تحلیل اطلاعات تخصصی و حرفه‌ای شده است. امروزه اطلاعات به شاخه‌های محلـی مسـتقل، اطلاعات تجاری، اطلاعات علمی، اطلاعات صنعتی و ... تقسیم شده است و داده‌ها به شدت تخصصی شده‌اند و موضوعات اطلاعاتی نیز بشدت تخصصی شده‌اند. مثلاً در چارچوب جنگ نرم و براندازی و

جاسوسی نرم انواع داده‌های فرهنگی، هنری و اقتصادی مهم شده‌اند. براین اساس سازمان‌های اطلاعاتی برای تفسیر و تحلیل این داده‌ها، توانائی کافی را ندارند. (حاجیانی،۱۳۹٦:۱۳٦).

چالش‌های حوزه اقدام پنهان در عصر اطلاعات

اقدام پنهان در کنار جاسوسی، یک شاخص اصلی فعالیت‌های اطلاعاتی به مفهوم عام آن می‌باشد. برخی از اندیشمندان اطلاعاتی و امنیتی آن را گزینه سوم بین دیپلماسی و نبرد آشکار می‌دانند. پهنه اقدام پنهان نیز با تحولات فنی، تغییرات محیط و تفکرات حاکمیتی دچار فراز و فروهایی بسیاری گردیده و با چالش‌هایی همراه شده است که برخی از این چالش‌ها عبارت‌اند از: (کلاهچیان،۱۳۹۳:۳)

۱- ایجاد قطب بندی اطلاعاتی و رقابت بر سر اطلاعات

قطب بندی‌های اطلاعاتی در دو بستر کشورهای پیشرفته و کشورهای در حال پیشرفت نمود بیشتری یافته و رقابت اطلاعاتی از سطح یک کشور، دولت، ملت به سطح اتحادیه‌های منطقه‌ای و تبادل دستگاه‌های اطلاعاتی این اتحادیه و رقابت با سایر اتحادیه‌ها تبدیل می‌شود. این عمل در حقیقت خط چین گشتن مرزهای کشورها و کمرنگی آنان را در پر رنگ نمودن اتحادیه‌های منطقه‌ای شکل می‌دهد.

۲- نسبت اقدامات پنهان و آشکار:

با توجه به انقلاب ارتباطات و اطلاعات، این نسبت به‌صورتی در می‌آید که اقدامات آشکار سطح بیشتری از فعالیت‌ها را در برگرفته نسبت بسیار کمتری به اقدامات پنهان داده می‌شود. در حقیقت در عصر کنونی شاهد کمرنگ شدن اقدام پنهان در سطح دولتی خواهیم بود و در حد عدم انجام تنزل می‌یابد. و به عبارت دیگر می‌توان اذعان داشت که اقدام پنهان توسط نیروهای هژمون کشورهای پیشرفته در یک بستر خاکستری از حالت نیمه پنهان به سمت آشکار در حرکت است. شاید یکی از بسترهای الزام این امر، فرایند قوه مقننه در کنترل اقدام پنهان باشد تا عملاً موجب رها شدن این اقدامات از سوی سازمان‌های اطلاعاتی گردد.

۳- تبدیل اقدام پنهان به عملیات پنهان در کشورهای رو به توسعه

با محدود شدن دولت‌ها و کم رنگ شدن مرزهای حاکمیت، سطوح غیر دولتی فعال شده عملیات پنهان به شکل نمادین حرکت‌های آزادیبخش یا با صبغه خشونت آمیز وارد عرصه جهانی می‌شوند در این میان، تهدید از سوی کشورهای در حال پیشرفت علیه کشورهای پیشرفته صورت گرفته و تکنولوژی به ابزاری جهت تهدید امنیت داخلی آنان مبدل می‌گردد.

٤- فرمالیسم (سطحی نگری، سطحی کارکردن، تظاهر)

از دیگر چالش‌های فراروی اقدام پنهان فرمالیسم است که بیشتر دولت‌ها نمایش این موضوع را تقبل می‌کنند، چراکه نظارت‌ها و کنترل‌های شدید، اساساً برای آنان راهی جز دیپلماسی پنهان بر جای ننهاده است. اقدام پنهان، با توجه به استرس ناشی از سرعت زیاد تغییرات، همه‌جانبه گرایی و همه‌جانبه نگری خود را ازدست‌داده و یا در یک دید خوش‌بینانه آن را کاهش می‌دهد. به عبارتی، در مقابل سرعت این تغییرات عقب می‌ماند و حالت ابزاری خود را برای حاکمیت ناکارآمد می‌کند. (ص، ۹۵:۱۳۸۵)

نتیجه‌گیری و پیشنهادها:

انقلاب اطلاعات و ارتباطات، جهان امروز را متحول ساخته است. فن‌آوری‌های نوین بر سرعت و سهولت تولید، توزیع و استفاده از اطلاعات افزوده است. انقلاب اطلاعات، شاید هیچ بخشی از بروکراسی دولتی را به‌اندازه سازمان‌های اطلاعاتی و سپس ساختار نظامی دست‌خوش تغییر و دگرگونی نساخته باشد. دلیل این امر تا حدود بسیاری مشخص است. زیرا حیات و کارکرد دستگاه‌های اطلاعاتی وابسته به اطلاعات است و حال چگونه می‌شود چرخه‌های اطلاعاتی در جوامع تغییرات اساسی را تجربه کنند اما سازمان‌های اطلاعاتی از آن متأثر نشوند. از طرف دیگر آنچه حجم و گستره این تأثیرپذیری را بیشتر ساخت، هم‌زمانی نسبی انقلاب اطلاعات با تغییر راهبردی جهانی به‌واسطه تغییر نظم جهانی ناشی از فروپاشی اتحاد جماهیر شوروی است. هم‌زمانی این دو رخداد با یکدیگر، یعنی تغییر نظم بین‌المللی و انقلاب اطلاعاتی، مباحثات گسترده‌ای را در دستگاه‌های اطلاعاتی کشورها برای ایجاد تغییرات ساختاری برپا کرد. در عصر اطلاعات عوامل تهدیدکننده متنوع و معادلات امنیتی پیچیدگی بیشتری یافته‌اند. این تغییرات لزوم بازنگری در ساختارها و عملکردهای دستگاه‌های اطلاعاتی و امنیتی برای مقابله با تهدیدات و چالش‌های جدید را می‌طلبد. در راستای انطباق این سازمان با شرایط جدید و پیچیده کنونی موارد زیر در قالب پیشنهادها تخصصی قابل‌طرح است:

۱- چابک سازی سازمان‌های اطلاعاتی و امنیتی به‌منظور تسریع در انطباق‌پذیری ساختارها با تغییرات جدید

۲-اولویت‌دهی به اقدامات تهاجمی و پیش‌دستانه اطلاعاتی در مقابله با پدیده‌های ناهمگن

۳-بازنگری در چرخه اطلاعات متناسب با شرایط جامعه شبکه‌ای و با تأکید بر سرعت و دقت در

فرآیند اقدامات اطلاعاتی

٤–اشرافیت بر محیط امنیتی خودی از طریق شناسایی نقاط قوت و ضعف و آسیب‌ها و تهدیدات نوین

۵–تقویت حوزه سایبری در سازمان‌های اطلاعاتی و امنیتی از طریق بـه‌کارگیری نیـروی انسـانی متخصص و فراهم ساخت زیرساخت‌های فناورانه

٦–تقویت منابع و ابزارهای پایش اطلاعاتی

۷–مهارت محوری و بهره‌گیری از توان هوشی و تحلیلی کارکنان سامانه‌های اطلاعاتی و امنیتی در جنگ اطلاعاتی

۸– تمرکز بر تولید اطلاعات راهبردی و شناسایی بسترها و کانون‌های آسیب‌زا

۹–پیوند با تکنولوژی‌های روز دنیا و رصد مستمر تغییرات نوین در عرصه فعالیت‌های پنهان

منابع

افتخاری، اصغر و قدرت‌آبادی، علیرضا(۱۳۹۵). نقش سازمان‌های اطلاعاتی در تأمین امنیت نرم، پژوهش‌های حفاظتی – امنیتی، ۵(۱۷)

پیرمحمدی، مهدی(۱۳۹۰). سازمان‌های اطلاعاتی و سیاست خارجی: مطالعه موردی نقش سازمان سیا در سیاست خارجی آمریکا. پایان نامه دکتری دانشکده حقوق و علوم سیاسی دانشگاه تهران، تهران: ابرار معاصر.

حاجیانی، ابراهیم و حاجیانی، مجید(۱۳۹٦). کارکرد سازمان‌های غیردولتی (مردم نهاد) در مردمی کردن اطلاعات، اطلاعاتی حفاظتی جامعه اطلاعاتی، ۸(۱)

دیو سالار، عبدالرسول(۱۳۹٤). بازخوانی تاثیرات متقابل سازمان‌های اطلاعاتی و سیاست در عصر اطلاعات، نقد کتاب، ۲(۷–۸)

زارعی، علی اصغر و واحدی، مرتضی(۱۳۸٦). جهانی شدن و سازمان‌های اطلاعاتی کشورهای توسعه یافته و در حال توسعه، مطالعات دفاعی استراتژیک، شماره ۲۹

شریف، عاطفه(۱۳۸۷). چالش‌های اطلاعاتی در گفتمان امنیت ملی، اطلاع شناسی، شماره ۱۹

قاضی‌زاده، علیرضا(۱۳۹۲). تأثیر جامعه شبکه‌ای بر فعالیت سازمان‌های اطلاعاتی، در کتاب اطلاعات به‌مثابه علم (درآمدی آینده‌پژوهانه بر مطالعات اطلاعاتی)، به اهتمام مهدی میرمحمدی، تهران: انتشارات پژوهشکده راهبردی.

کلاهچیان، محمود(۱۳۹۳). مدیریت عملیات پنهان، پژوهش‌های حفاظتی – امنیتی، ۳(۱۱)

گادسون، روی و آر می، ارنست و اشمیت، گری(۱۳۸٤). اطلاعات آمریکا بر سر دوراهی، ترجمه معاونت پژوهشی دانشکده امام باقر (ع)، تهران: انتشارات دانشکده امام باقر (ع).

گنجی دوست، محمد(۱۳۸۷). تحولات دیپلماسی در عصر اطلاعات، سیاست، دوره ۳۸، شماره ۱

م.ص(۱۳۸۵). بررسی چالش‌های اقدام پنهان در عصر جهانی شدن، پژوهش‌های اطلاعاتی – امنیتی، شماره ویژه جامعه اطلاعاتی.

معاونت پژوهش و تولید علم(۱۳۹۳). رویکردهای نظری به ضد اطلاعات، تهران: موسسه چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی.

معاونت پژوهش و تولید علم(۱۳۹۵). چالش‌های اطلاعاتی در جهان معاصر، تهران: موسسه چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی.

نجفی، محسن و پسندیده، جواد(۱۳۹۹). سازمان‌های مردم نهاد؛ حوزه‌های تأثیر بر امنیت و اطلاعات، تهران، مرکز مطالعات و پژوهش‌های اطلاعاتی معاونت اطلاعات آجا: انتشارات مرکز آموزشی وپژوهشی شهید سپهبد صیاد شیرازی.

ولز، گلن و مرن، لیندزی و فیلپات، دان(۱۳۹۳). ضد اطلاعات و حفاظت عملیاتی، ترجمه معاونت پژوهش و تولید علم، تهران: موسسه چاپ و انتشارات دانشکده اطلاعات.

هدایتی، علی رضا(۱۳۹۳). جمع‌آوری آشکار در عصر اطلاعات، تهران: موسسه چاپ و انتشارات دانشکده اطلاعات.