راهبردها و الزامات هوش امنیتی در جنگ ترکیبی

محمد کاویانی[1]، علی جلالی[2]

چکیده

هدف این پژوهش شناسایی راهبرد و الزامات هوش امنیتی درمقابله با جنگ ترکیبی است. تحقیق حاضر که به لحاظ هدف، کاربردی؛ به لحاظ روش استنتاج، توصیفی و به لحاظ ماهیت داده‌ها، کیفی و کمی است؛ در سه مرحله اصلی انجام شده است. در مرحله اول، با استفاده از روش نمونه‌گیری نظری، با ۱۲ نفر از صاحنظران مصاحبه‌های نیمه ساختاریافته به عمل آمد. سپس، با کمک نرم افزار MAXQDA ، داده‌ها تحلیل و در طی کدگذاری باز ۴۸ مورد به عنوان مفاهیم اولیه از متن مصاحبه‌ها شناسایی شد که در قالب ۱۰ شاخص فرعی و ۲ شاخص اصلی دسته بندی شد. در بخش کمّی پژوهش، در مرحله دوم به منظور تعیین درجه اهمیت راهبردهای امنیت در هوش امنیتی از روش آنتروپی شانون، و در مرحله سوم به منظور رتبه بندی راهبردهای مذکور، از روش ماباک، استفاده گردید. نتایج تحقیق نشان داد که الزامات تخصصی هوش امنیتی، الزامات تعاملی هوش امنیتی، الزامات مواجهه با دشمن، الزامات شرعی و قانونی، الزامات فردی و خودسازی و الزامات بکارگیری هوش امنیتی، به ترتیب بالاترین درجه اهمیت را در میان الزامات هوش امنیتی در جنگ ترکیبی، کسب کردند. همچنین، نتایج تحقیق نشان داد که بهبود زیرساخت هوش امنیتی، بهبود هوش امنیتی تاکتیکی، طراحی سامانه هوش امنیتی راهبردی و مدیریت افکار امنیتی سازمان، به ترتیب بالاترین رتبه را در میان راهبردهای بهبود هوش امنیتی درمقابله با جنگ ترکیبی، به خود اختصاص دادند. پیشنهاد کاربردي تحقیق تحت عنوان پیاده سازی مواردا‌حصاء شده هوش امنیتي‌درمقابله با جنگ ترکیبی مدنظر مي باشد.

واژگان کلیدی: امنیت، هوش امنیتی، الزامات هوش امنیتی، راهبردهای هوش امنیتی ،جنگ ترکیبی

---

۱ . مدرس دانشگاه افسری و تربیت پاسداری امام حسین (ع)؛

۲ . عضو هئیت علمی دانشگاه افسری و تربیت پاسداری امام حسین(ع).

مقدمه

بحث درباره امنیت، از دشواری‌های متنوعی برخوردار است که از جمله می‌توان به معنای امنیت و مرزهای نامعلوم آن در مفاهیمی همچون امنیت جامعه، امنیت جمعی، امنیت انسانی، امنیت ملی، امنیت سازمانی و غیره اشاره نمود. برخلاف گذشته که امنیت، امر عینی و واقعی بود؛ امروزه مفهوم امنیت بیشتر ذهنی و مبتنی بر تصمیم بازیگران است(فام و دیگران[1] ۲۰۱۹).

در این فضاي به شدت پیچیده و متلاطم، افراد، سازمانها و ملتها در معرض هجوم تغییراتي بیش ازاندازه و خیلي سریع قرار گرفته اند که باعث آشفتگي و از دست دادن ظرفیت آنها براي اتخاذ تصمیم‌هاي هوشمندانه و انطباق پذیر شده است(تافلر، (۴ ،۱۳۷).

با افزایش حجم رخدادهاي امنیتی وشناسایی تهدیدات و حملات داخلی و خارجی توسط ابزارهاي امنیتی نیاز است با رویکرد امنیتی وحفاظتی، بتوان رخدادها و داده هاي گزارش شده را مانیتورینگ کرده و بین آنها ارتباط برقرار نمود و از این طریق تهدیدها و آسیب‌ها را تحت کنترل قرارگیرند(انسی وهمکاران۱۳۸۸ص۲۳۷).

ویژگي‌هاي انسان به ویژه هوش و فعالیت‌هاي هوشمندانه همواره موردتوجه اندیشمندان بوده است. واز دیدگاه‌هاي گوناگون به تعریف، طبقه بندي وسنجش هوش پرداخته اند.اگرچه تا سال‌ها ، منظور از هوش ، هوش عقلاني یا منطقي مدنظر بود است. اما امروزه در تعریف هوش موارد دیگري ازجمله هوش عاطفی،سازمانی،هیجانی،استراتژیک ،معنوی، اجتماعی و...مطرح شده است. از این رو، مدیران در سازمان‌ها علاوه بر هوش‌های مطرح شده،باید دارای هوش امنیتی با قابلیت‌های امنیتی، حفاظتی ومهارت‌های ارتباطی برخوردار باشند. زیرا اهمیت و ارزش آن می طلبد، به مثابه یک رشته مستقل درکنار سایر هوش بیان نماییم.

واقعیت‌های راهبردی موجود نشان می دهد ، دستیابی به اهداف کلان ملی بدون داشتن اطلاعات اساسی و کلیدی از روندهای موجود ، مبانی و تنگناهای رقابتی آینده محقق نخواهد شد لذا یافتن سیاست‌های کلان امنیتی ازجمله شناخت شیوه‌ها و کارکردهای هوش امنیتی در سطح ملی بخصوص درساختارحاکمیتی و اجرای دانش‌های امنیتی زمینه ساز رسیدن به این هدف مهم و کلیدی می باشد .در این میان شناسایی الزامات هوش امنیتی ورتبه بندی راهبردهای آن در ساختارهای حاکمیتی می تواند منجر به تصمیم سازی مناسب سازمانی منطبق با هوش امنیتی را فراهم نماید(ملکی فر ۱۳۸۶ : ۱۸) .

---

1. Pham et al

در این بین، تهدیدات امنیتی می‌تواند ثبات و پایداری سازمان‌ها را با تأثیرگذاری بر محرمانه بودن، یکپارچگی و در دسترس بودن سرمایه اطلاعاتی/ ساختاری، مختل کنند. نمونه‌هایی از این پتانسیلِ ایجاد اختلال و اثرات خارجی، شامل سقوط سازمانی، تا ناتوان ساختن زیرساختهای کشورهاست (کیسر[1] ۲۰۱۵).

با اینکه هنوز شناسایی الزامات امنیتی و راهبردهای آن به صورت یک بسته جهت مدل هوش امنیتی درجنگ ترکیبی ناشناخته است. بررسی چگونگی انتخابات دیدگاه و رویکرد مناسب هوش امنیتی در این میان بسیار اساسی است .که با تبیین الزامات وراهبردهای امنیتی منجر به قابلیت پیشرانه‌های کلیدی درکارآمد سازی مقابله با جنگ ترکیبی[2]وعدم غافلگیری مدیران درآینده خواهدشد.

بیان مساله

عصر اطلاعات وچالش‌های فراروی آن، فرصت‌ها و تهدیدات جدیدی را مطرح کرده است که تنها سازمان‌ها، با مدیرانِ دارای تفکر مؤثر امنیتی، قادرهستند نقاط قوت، ضعف و فرصتهای محیطی راشناسایی و به تهدیدات پیرامونی پاسخی قاطع دهند.(عاطف (۱۵:۱۳۷۸)در ساختار حاکمیت مدیران ارشد باید بدانندکه از سوی چه افراد، سازمانها ،ابزارهای فنی و... مورد تهدید قرار می گیرد تا بتوانند منابع خود رابرمهمترین مسائل متمرکزکنند.(اکبرزاده۲۸:۱۳۸۳)

راهبردهای امنیتی سازمان، ریشه در یک سناریوی "جنگ ترکیبی" ادامه دار دارند، که برخلاف "نبردهای" فردی، به طور قطعی نمی‌توان درآن برنده شد. به عبارت دیگر، امنیت مسئله‌ای نیست که بتوان آن را برای همیشه "حل" کرد(سالوس و دیگران، ۲۰۱۹). در این بین، ذینفعان سازمانی مانند کارکنان و مدیران، ممکن است قوانین و راهبردهای امنیتی را به طور متفاوت درک کنند. ادبیات موجود نشان می‌دهد که ادراک ذینفعان از هوش امنیتی می‌تواند به موفقیت یا شکست راهبردهای سازمان،کمک کند(ساموناس و دیگران، ۲۰۲۰).از این رو، مدیران مدنظر در سازمان‌ها باید دارای قابلیت امنیتي بوده، که از توانمندي‌هاي اطلاعاتي، امنیتي و مهارت‌هاي ارتباطي برخوردار باشند. زیرا اهمیت وارزش کاربرای این حوزه اقتضاء داردآن را به مثابه یک رشته مستقل از عناوین پژوهشی خاص تعریف نماییم(اکبرزاده،۲۸:۱۳۸۳).

مساله اصلی هوش امنیتی وبیان الزامات و راهبردهای آن در جنگ ترکیبی این بوده که از سوی افراد، سازمانها ،ابزارهای فنی و... همواره مورد تهدید قرارمی گیرد که یا شناخت و اولویت بندی

---

1 . Kaiser
2 . Combined war(hybrid)

تهدیدات سازمانی (مدیریت تهدیدمحور) از جمله رویدادها، روندها، آسیب‌ها و توجه به جریان نفوذ در بدنه حاکمیت از طریق مدیرانی بارویکرد هوش امنیتی مثمر ثمرخواهد بود.واین موضوع به دنبال این گزاره بوده که هر ساختارحاکمیت بدون داشتن راهبردهای امنیتی دچار مخاطرات امنیتی خواهد شد.

اهمیت

پژوهش حاضر، با واکاوی عقاید و دیدگاه‌های صاحب نظران؛ ایجاد یک دید جامع و راهبردی در جهت تشخیص، حفاظت و مدیریت تهدیدات امنیتی را از طریق شناسایی الزامات و راهبردهای امنیتی بر اساس مدل هوش امنیتی در جنگ ترکیبی؛ مورد بررسی قرار می دهد.

ضرورت

عدم انجام این تحقیق موجب می‌گردد تا در جنگ ترکیبی، به ویژه موارد مرتبط با سازمان‌های اطلاعاتی و امنیتی دچار غافلگیری شویم.

سؤال‌ها و فرضیه: پژوهش حاضر فرضیه آزما نیست. سوالات محققان عبارت است از:

۱. الزامات و راهبردهای هوش امنیتی در جنگ ترکیبی کدامند؟
۲. چه راهبردهایی جهت بهبود هوش امنیتی در جنگ ترکیبی می‌توان اتخاذ نمود؟

پیشینه پژوهش

امروزه مزیت رقابتی سازمان‌ها در مقدار دانایی، هوش، شایستگی و دانش خردمندانه نیروی انسانی آن‌ها پنهان است. برای تبیین تعریفی جامع از هوش، تلاش‌هایی صورت پذیرفته که همواره با مناقشه و مشکل همراه بوده است. این امر به این دلیل است که هوش، مفهومی است انتزاعی و درحقیقت پایه محسوس فیزیکی و عینی ندارد. هوش برچسبی کلی برای مجموعه‌ای از فرایندهاست که از پاسخ‌های آشکار و رفتار افراد برداشت می‌شود (نجفی شهرضا و دیگران، ۱۳۹۹).

برای اولین بار در اوایل قرن بیستم، آلفرد بینت[1]توانست هوش ریاضی یا بهره هوشی (IQ) را به دنیا معرفی کند. به نظر وی، هوش ریاضی زیاد تضمین کننده فرایند بسیار مؤثر به یادسپاری ارقام است (باقری و دیگران، ۱۳۹۱). در همین رابطه، هوارد گاردنر وهاتچ[2](۱۹۹۰) هشت شکل مختلف از دانش را ارائه نمود که به اعتقاد وی تصویری جامع‌تر از هوش را بیان می‌کند که عبارت است از: هوش زبانی ـ

1.Alfred Binet
2. Gardner & Hatch

کلامی، منطقی ـ ریاضی (اعداد و ارقام)، تصویری ـ فضایی (ایجاد تصویری ذهنی از واقعیت و تغییر بی درنگ و آسان آن)، موسیقیایی یا آهنگینی (توانایی درک و ایجاد الگوهای آهنگینی و نواختی)، جسمانی-حرکتی (مهارت عضلانی و حرکت جنبشی مناسب)، طبیعت‌گرا، میان‌فردی (توانایی درک دیگران و نحوه تعامل آن‌ها با یکدیگر) و درآخر، هوش درون‌فردی (توانایی درک و شناخت خویشتن) (گاردنر وهاتچ، ۱۹۹۰). گاردنر معتقد بود که باتوجه به دو شکل اول، سایر توانایی‌های ذهنی بشر نادیده گرفته می‌شود و فقط بخشی از توانمندی‌های انسان مدنظر قرار می‌گیرد (گاردنر[1] ۲۰۰۶).

بررسی پیشیه تحقیق نشان داد که به طور کلی، مطالعات متعددی پیرامون هوش و انواع مختلف آن به طور جداگانه صورت گرفته است، ولی آنچه که مشخص گردید این بود که تحقیقات انجام شده در رابطه با الزامات هوش امنیتی درطراحی مدل هوش امنیتی در مقابله با جنگ ترکیبی ، تاکنون مورد توجه پژوهشگران قرار نگرفته است. اما به برخی از تحقیقات انجام شده با موضوع هوش و امنیت اشاره می‌گردد.

مجتبي خدادادي و علي حسن پور(۱۳۹۲) درتحقیقی تحت عنوان"نقش هوش هيجاني در توانمندي امنيتي مديران" با جامعه آماري مديران عالي سازمان‌هاي امنيتي كشورانجام گرديده كه براين اساس انتظار مي‌رود مديراني كه از هوش هيجاني بالاتري برخوردارند، اثربخشي بالاتري نيز در مديريت داشته باشند.اين امر مي‌تواند در انتخاب مديران شايسته در سازمان هاي امنيتي مورد توجه باشد.

محمود كلاه چيان(۱۳۹۳) درتحقیقی تحت عنوان "مديريت عمليات پنهان درسازمان هاي امنيتي" بيان می دارد دير زماني است كه پهنه عمليات پنهان با تحولات فني، تغييرات محيط و تفكرات حاكميتي دچار فراز و فرودهاي چندي گرديده است.

فريبا شايگان(۱۳۹۱) درتحقیقی تحت عنوان" امنيت پايدار از ديدگاه مقام معظم رهبري" براي دستيابي به نظريات مقام معظم رهبري در خصوص امنيت پايدار چهار سؤال ويژگي امنيت پايدار، مشمولين آن، متوليان آن و نيز شيوه‌هاي ايجاد و حفظ آن مطرح شد.

جعفر فيني زاده بيدگلي وهمكارن (۱۳۹۵) درتحقیقی تحت عنوان "بررسی ویژگی امنیتی شدن یک پدیده (موضوع) درجمهوری اسلامی ایران" نتايج اين تحقيق مشخص می کند، بازيگران و ميزان جدي بودن تهديدات، بالاترين سهم در امنيتي شدن موضوعات ازجمله بحران‌ها را دارند.

---

1 . Gardner

آنچه که می‌توان در خصوص تاریخچه جنگ ترکیبی بیان داشت:

۱. مبدا جنگ ترکیبی جنگ درگیری بین روس وچچنی‌ها (سال۲۰۰۲) بوده است.
۲. جنگ بین روسیه و کریمه و شرق اوکراین را هم میتوان جنگ هیبریدی و ترکیبی نامید که در ان جنگ، اروپا از روسیه شکست خورد.
۳. جنگ ۳۳روزه(جنگ حزب الله بعنوان گروه جهادی ومقاومت علیه رژیم صهیونیستی).
۴. روسیه در داخل امریکا با دخالت در انتخابات ان کشور از جنگ ترکیبی استفاده کرده است.
۵. روسی‌ها با به‌راه انداختن جنگ هیبریدی در غرب بدنبال روی کار آوردن افراطی‌ها در غرب هستند.
۶. آشوبهای هنگ کنگ جنگ ترکیبی غرب علیه چین بوده است.

مبانی مفهومی

۱-۲.هوش

بررسی ادبیات نشان می‌دهد، از هوش تعریف واحدی به دست نیامده و صاحب نظران مختلف آن را به گونه‌های متفاوتی تعریف کرده‌اند. نمی‌توان تعریف مشخصی از هوش به دست آورد که مورد توافق همه روانشناسان وابسته به رویکردهای مختلف باشد. با این حال عناصری از هوش وجود دارند که مورد توافق غالب پژوهشگران است. این عناصر را با توجه به ادبیات، می‌توان در سه دسته تقسیم کرد (سیف، ۱۳۹۸).

توانایی پرداختن به امور انتزاعی: منظور این است که افراد باهوش بیشتر با امور انتزاعی (اندیشه‌ها، نمادها، روابط، مفاهیم، اصول) سروکار دارند تا امور عینی (ابزارهای مکانیکی، فعالیت‌های احساسی).

توانایی حل کردن مسائل: یعنی توانایی پرداختن به موقعیت‌های جدید، نه فقط دادن پاسخ‌های از قبل آموخته شده به موقعیت‌های آشنا.

توانایی یادگیری: به ویژه توانایی یادگیری انتزاعیات، از جمله انتزاعیات موجود در کلمات و سایر نمادها و نیز توانایی استفاده از آن‌ها.

۲-۲.امنیت

امروزه تعاريفي كه امنيت را وجود شرايط و انجام اقداماتي براي مصون نگه داشتن از اعمال نفوذ دشمن مي‌داند، ناقص و نارس است. از اين رو سخن والتر ليپمن كه مي‌گويد: هر ملتي تا جايي داراي امنيت است كه درصورت عدم توسل به جنگ مجبور به‌رها نمودن ارزشهاي محوري و اساسي خود

نباشد و چنانچه درمعرض چالش قرارگرفت بتواند با پیروزي درجنگ آنها راحفظ کند» (قریب : ۱۳۸۰: ۳۱).« امنیت » مفهومي چند وجهي و همزاد با مفاهیمي مانند قدرت، تهدید و آسیب است. تعاریف موجود در فرهنگ‌ها، امنیت را احساس آزادي از ترس یا احساس ایمني که ناظر بر امنیت مادي و رواني مي‌باشد تعریف مي کنند. امنیت با تعریف مفهوم مخالف یعني ناامني و بیان شاخص‌های وضعیت فقدان امنیت نیز تقریب به ذهن است »(شیدائیان، ۱۳۸۸: ۱۴).

۳-۲.هوش امنیتی

هوش امنیتی واطلاعاتی، می‌تواند رخدادها و داده‌های گزارش شده را شناسایی و رصد کرده و بین آن‌ها ارتباط برقرار نموده و از این طریق، تهدیدها و آسیب‌ها را شناسایی تا تحت کنترل اطلاعاتی وامنیتی، قراردهد(رضایت و مرادیان، ۱۳۹۵).

پیرک و دیگران[1](۲۰۱۶)، هوش امنیتی را جمع آوری، به هنجارسازی، همبسته سازی و تحلیل بزرگ داده‌های امنیتی یک سازمان که از طریق کاربران، برنامه‌های کاربردی و زیرساخت‌ها، ایجاد شده است و روی امنیت و مدیریت مخاطرات فناوری اطلاعات در سازمان تأثیر می‌گذارد، تعریف کرده و معتقدند، هوش امنیتی به دنبال مدیریت همه جانبه اطلاعات امنیتی در سازمان است. (پیرک و دیگران، ۲۰۱۶الف). آنچه مشخص است هوش امنیتی دو بخش مهم و اساسی را پوشش می‌دهد؛ یک بخش مربوط به مدیریت تعاملات و همبستگی فناوری‌های مورد استفاده در امور امنیتی سازمان و دیگری، مدیریت یکپارچگی و همبستگی این اطلاعات (ساموناس و دیگران[2]، ۲۰۲۰).

هوش امنیتی، یک بستر مدرن، هوشمند و کارآمد برای تأمین امنیت سیستمها و بسترهای مبتنی بر اطلاعات و شبکه است که با ایجاد یک مانیتورینگ مستمر از تمامی تجهیزات و دستگاه‌ها و جمع آوری تمامی لاگ‌ها، کانفیگ‌ها[3]، رویدادها و گزارشات اخذ شده از این تجهیزات و دستگاه‌ها بصورت مبتنی بر عامل یا بدون عامل (مستقل)، پس از عملیات‌های نرمال سازی و تجزیه و تحلیل، گروه بندی و همبسته سازی، اضافه کردن اطلاعات زمینه، الویت بندی بر اساس میزان مخرب بودن، بطور خودکار تهدیدات و ریسک‌های امنیتی را تشخیص و از بروز حملات جلوگیری می‌نماید(مانوگران و دیگران[4]، ۲۰۱۷).

1.Pirc et al
2.Samonas et al
3.Configures,
4. Manogaran et al

مفهوم گرگهای تنها: به شخص ویا تعدادمحدودی از اشخاص گفته میشودکه به تنهایی وبدون اینکه با گروهی از بازیگران ثالث(سرویس،گروهکهای مسلح وبرانداز،فرقه‌های انحرافی،اراذل و اوباش وگرههای مذهبی) ارتباط (سازمانی و اگاهانه ویا از انها کمکی دریافت کرده باشند) داشته باشند،در ایجاد ناامنی و اغتشاش ایفای نقش میکنند. گرگهای تنها در اغتشاشات:گرگهای تنها در تمام اغتشاشات از سال ۱۳۹۵فعال شدند (بصورت سازماندهی شده و تیمی)در را اندازی‌های اغتشاش و نا امنی‌های شدید ایفای نقش کرده ودست به اقدامات خشونت امیز میزنند.

۴-۲.جنگ ترکیبی

تهدیدات دهه ۶۰ تهدیدات سخت و اغلب آن نیمه سخت بودند ولی تهدیدات دهه۷۰ غالبا نیمه سخت یا نرم (تهاجم فرهنگی) بوده اند و تهدیدات دهه۸۰ اغلب هوشمند(کودتای مخملی، انقلاب رنگی، فتنه۸۸ و.....) توضیح اینکه فتنه ۸۸ تیر خلاص به تهدید هوشمند بوده است تهدیدات دهه۹۰ جنگ هوشمند از اواخر سال۹۵ (اواخر دولت اوباما شروع شده که می گوید ما در ایران تغییر رژیم نداریم بلکه تغییر رفتار داریم) جنگ ترکیبی شروع شده ولی درسال ۱۴۰۰ مقام معظم رهبری آنرا مطرح کردند یعنی همین تغییر رفتار نتیجه‌اش تغییر رژیم هم است منتهی در تغییر رفتار ظاهرش خیلی قابل تشخیص نیست (حذف ولی فقیه، محدودشدن در لبنان، سوریه و عراق و.....) همین که ترامپ وقتی نتیجه کارش را در برجام گرفت دوباره گرفت دوباره تغییر رژیم را مطرح کرد.

تهدید هوشمند: ترکیبی از تهدیدات نرم ونیمه سخت با اغلب تهدیدات نرم بوده روندی که دشمن در جنگ ترکیبی پیش و دو گرفته نتایج حاصله توسط دشمن قابل توجه است.

قبل ازسال ۹۵ سازماندهی اعتراضات به صورت عمودی و سلسله مراتبی بودند ولی از سال ۹۵ به بعد سازماندهی اعتراضات به افقی(جمعیت پایه با ایفای نقش جوانهای ناراضی در جامعه که در فضای مجازی جذب و سازماندهی در گروهای جوک سرگرمی، اخلاقی، ورزشی، هنری، موسیقی، عاشقانه، همجنس‌گرا، ازدواج سفید، هوادارمحیط زیست و حتی گروههای مذهبی می شوند).

مفهوم جنگ ترکیبی،تهاجم ترکیبی وجهاد تبیین این مفاهیم شبیه کلید واژه مورد استفاده تهاجم فرهنگی، شبیخون، غارت و ناتوی فرهنگی دهه هفتاد می‌باشد که آن موقع مقام معظم رهبری تکرار و تاکید داشته ولی جدی گرفته نشد. دیروز هم خیلی از نیروهای خودی سرگردان بودند بطوری که برخی می گفتند که تبادل فرهنگی داریم یا تهاجم فرهنگی لذا باعث سردر گمی و حتی فراموش شدن اصل قضیه شده است تا جائیکه در کل بیشتر کار فقط به زن یک عکس، نوشته و تصویر روی لباس و آدامس و...خلاصه شده است. علت اصلی سردر گمی عدم توجه به اطلاعات پنهان و تحلیل سطحی بوده است. در بحث تهاجم ترکیبی و جهاد تبیین هم اینگونه است یعنی فقط به شواهد و قرائن اشکار اکتفا

می‌شود به راهبرد دشمن و اطلاعات پنهان (اطلاعات پنهان اطلاعات) توجه نمی‌شود. (کاتوزیان۱۳۷۲).

تعریف اول : ترکیبی از چند جنگ است، جهت هم افزایی وتشکیل یک جنگ.در صورتیکه هیچ کدام از جنگ‌ها نیست مثل اب و شکر وقتیکه که مخلوط می‌شوند نه اب است و نه شکر.

در جنگ ترکیبی اگر شناخت مولفه ، ابعاد، روند، ابزار وعوامل جنگ خوب شناخته شده و مدیریت شود تبدیل به فرصت می‌شود این قضیه همان مطلبی است که رهبری فرمودند پیچ تاریخی که زمینه ای برای تمدن اسلامی است.

تعریف دوم:(تعریف ازنگاه دشمن): ترکیبی از نبرد متعارف (کلاسیک که در جبهه در مقابل هم هستند) و نا متعارف (چریکی و نامنظم دو طرف در درون هم هستند) است.در مقایسه نبرد متعارف ونامتعارف شاخص‌های موردتوجه هستند. (عمادی۱۳۹۸ص۲۰)

اهداف جنگ ترکیبی از زبان مهاجمین، سه هدف اصلی مطرح شده است:

۱. تاثیرگذاری روی سیاستگذاری نظام؛
۲. زمینه سازی برای حمله نظامی؛
۳. تصرف قلمرو بدون بکارگیری انبوه نیروهای نظامی .

جنگ ترکیبی: ترکیبی از تهدیدات نرم، نیمه سخت و سخت بطور همزمان وهماهنگ علیه مولفه‌های قدرت، درصورتیکه درجنگ هوشمند اولویت جنگ نرم است، خیلی از براوردهای تهدیدات از منظراطلاعات آشکار خودمان است نه از منظر دشمن که می بایست از اطلاعات پنهان باشد(براوردی که از اطلاعات آشکار باشد براورد غلطی است)(عمادی،۱۳۹۸،ص۱۴).

گرگهای تنها درجنگ ترکیبی:

به گروههای خفته متصل(نه وابسته) به بازیگران ثالث و برخوردار از آموزش آشوب(معمولا در فضای مجازی) و قادر به تحرک‌بخشی جوانان ناراضی،معترض وماجراجو گفته می‌شود.

ویژه‌گی‌های گرگهای تنها:

۱. از خانواده‌های آسیب پذیرند؛
۲. تحت عناوین خاصی جذب می‌شوند؛
۳. به صورت مرحله ایی تبدیل به یک آتش زیر خاکستر می‌شوند؛
۴. زمانی وارد میدان می‌شوند که زمینه‌های لازم اجتماعی،اقتصادی و....وجود داشته باشد و عملکرد نابجا وحساب نشده و بعضا غلط دستگاها بهانه ایی برای حضور انها را بدهد.

۳.مبانی نظری و الگوی تحلیل

۱-۳.مولفه‌های هوش امنیتی

بطور کلی می‌توان گفت هوش امنیتی، جمع آوری، هنجارسازی، همبسته سازی و تحلیل بزرگ داده‌های امنیتی یک شبکه به منظور خودکار کردن فرآیندهای کاهش سطح مخاطرات آن شبکه با تبدیل میلیون‌ها بسته اطلاعاتی به یک اقدام عملی آنی می‌باشد(کرمپ[1] ۲۰۱۵).

ادبیات موجود نشان می‌دهد که هوش امنیتی دارای سه جز اصلی ۱.مدیریت اطلاعات و رخدادهای امنیتی[2] ۲.مدیریت ریسک[3] و ۳.انطباق قوانین[4] است(پیرک و دیگران[5] ۲۰۱۶ب):

مدیریت اطلاعات و رخدادهای امنیتی؛ به عنوان قلب هوش امنیتی در مقابله با جنگ ترکیبی به شمار می‌آید؛ زیرا، زیرساخت اصلی هوش امنیتی توسط این بخش تأمین می‌گردد و از دو بخش مدیریت اطلاعات امنیتی و مدیریت رخدادهای امنیتی، تشکیل شده است. مهم‌ترین وظایف بخش مدیریت اطلاعات و رخدادهای امنیتی عبارت است از مدیریت لاگ[6] یا نگاشت، نرمال سازی[7] یا هنجار سازی، همبسته سازی رویدادها[8] عکس العمل آنی به تهدیدات (پاسخ فعال[9])، امنیت عناصر انتهایی (EPP)؛[10] ذخیره سازی وقایع[11] و ارائه گزارشات تحت وب.[12]

مدیریت ریسک: هدف مدیریت ریسک یا مدیریت مخاطرات در هوش امنیتی، کاهش زیان‌های ناشی از عملی شدن تهدیدات می‌باشد که با استفاده از سه شاخص شناسایی، ارزیابی و اولویت گذاری بر مبنای استاندارد مدیریت ریسک در پنج گام می‌توان به این هدف رسید که عبارت است از:۱-تشخیص و شناسایی تهدیدات ۲-ارزیابی آسیب پذیرهای هدف تهدیدات ۳-تشخیص زیان‌های ناشی از عملی شدن تهدیدات ۴-تعیین راهکارهای کاهش مخاطرات و ۵-اولویت گذاری راهکارها.

1.Crump
2. Security Information and Event Management
3.Risk Management
4.Regulatory Compliance
5.Pirc et al
6.Log
7.Normalization
8. Event Correlation
9.Active Response
10.Endpoint Protection Platform
11.Event/Incident Storage
12.Web-based Reports

انطباق قوانین: هدف انطباق قوانین در هوش امنیتی، حصول اطمینان از برقراری سه مورد تطابق با استانداردها (استفاده از استانداردها در پیاده سازی هوش امنیتی، همچون استفاده از استاندارد ISO 50772 در پیاده سازی مدیریت ریسک در هوش امنیتی در مقابله با جنگ ترکیبی)، پایداری در نظارت (نظارت و مانیتورینگ مستمر و دائمی هوش امنیتی بر کلیه فعالیت‌ها و رویدادها) و کامل بودن بازرسی (بررسی همه جانبه و تجزیه و تحلیل کامل کلیه فعالیت‌ها و رویدادها توسط هوش امنیتی).

۲-۳.اصول هوش امنیتی

سه جزء تشکیل دهنده هوش امنیتی، شامل مدیریت اطلاعات و رخدادهای امنیتی، مدیریت ریسک و انطباق قوانین، بر مبنای سه اصل "هوش، یکپارچگی و خودکار سازی" با هم در تعامل بوده تا هدف اصلی هوش امنیتی که تأمین امنیت است تحقق یابد. هوش امنیتی با ایجاد مانیتورینگ و نظارت مستمر و دائمی بر کلیه فعالیت‌ها و رویدادهای سازمان مربوطه و بررسی و تجزیه و تحلیل این فعالیت‌ها و رویدادها هرگونه ناهنجاری و تهدید را شناسایی و از بروز حملات امنیتی جلوگیری می‌نماید(پیرک و دیگران،۲۰۱۶ب).در این راستا شناخت راهبردهای هوش امنیتی زمینه ساز تحقق الزامات آن است.هوش امنیتی راهبردی[1]درسطح بالای تصمیم گران مورد استفاده قرار می گیرند.

۳-۳.جنگ ترکیبی

استراتژیست و فیلسوف نظامی سان تزو معتقد است؛ برای مبارزه؛ تصرف در تمام جنگ اقدام چندان عالی نیست؛ بلکه برتری اصلی، «شکستن مقاومت دشمن بدون جنگ است». نتیجه منطقی این است که دیدگاه مفهومی در مورد جنگ‌های ترکیبی در مفاهیم علوم سیاسی و نظامی شرق از سوی کاتیلا و سن تزو وجود داردو توسط نظریه پردازان بعدی بازتولید شده است (قربانی زواره، ۱۳۹۸: ۱۳۴).

استفاده از شورش‌ها و ناآرامی‌های اجتماعی به عنوان یک عامل ایجاد بی‌ثباتی نقش مهمی در جنگ ترکیبی ایفا می‌کند. نوآوری جنگ ترکیبی این است که نیروهای منظم و نامنظم می‌توانند هم‌زمان وارد یک درگیری فعال اجتماعی، دستکاری شده یا اجباری علیه یک جمعیت مشخص شوند. در عین حال انواع اقدامات از جمله"تغییر رژیم" و " مهندسی دموکراسی" ، همراه با استفاده ابزاری از موضوع صلح، می‌توانند برای دستیابی به اهداف اجتماعی و سیاسی استفاده شوند.از این نظر، جنگ ترکیبی غالبا از روش‌های قانونی و غیر قانونی و هم اقدامات نظامی و هم غیر نظامی استفاده می‌کند که به طور مستقیم بر جمعیت هدف تاثیر گذاشته و واد منازعه با آن می‌شود (Gardner 2015).

---

1 . Strategic security intelligence

ایالات متحده آمریکا، تمامی منابع سه گانه قدرت را در ابعاد اقتصادی، امنیتی، فرهنگی، علیه دشمنان خود به خدمت گرفته است و گویی یک مثلث قانم‌الزاویه که راس آن امنیت است را تشکیل داده است. NPT،JCPOA ، CAATSA و CTBT در راس آن مثلث (امنیت)، ISAو FATF در زاویه اقتصاد و سند ۲۰۳۰ یونسکو و مصوبات کنگره آمریکا هم در زاویه فرهنگی آن، عمل می‌کنند. مهمتر اینکه این ابعاد کاملا در هم تنیده هستند به عبارت دیگر امکان ایجاد یک راهبرد ترکیبی را می‌دهند که در آن انقلاب در امور نظامی و انقلاب رنگی با هم نمود پیدا می‌کند. (عسگرخانی، ۱۴۰۰، مقدمه کتاب جنگ‌های ترکیبی، نوشته اندرو کوریبکو، ترجمه سبحان محمدی)

۴-۳.راهبردهای بهبود هوش امنیتی درمقابله با جنگ ترکیبی دشمن شامل؛

بهبود زیرساخت، بهبود هوش امنیتی تاکتیکی، طراحی سامانه هوش امنیتی راهبردی ومدیریت افکار امنیتی بوده که این اطلاعات به ندرت شامل موارد فنی هستند و بر اطلاعات مرتبط با ریسک تمرکز دارند. از جمله چیزهایی که در این اطلاعات می توان یافت موارد مرتبط با تاثیر مالی رخداد سایبری، روندهای حملات آتی، حوزه‌های مستعد برای حمله مهاجمان و حوزه اثرگذار بر تصمیمات کلان و سطح بالای سازمان می باشد. چنین اطلاعاتی به سازمانها در تعیین اقدامات، ظرفیت‌ها و بودجه لازم را برای مقابله و کاهش خطر حملات احتمالی کمک می کند. هوش امنیتی راهبردی اغلب به صورت خبر و اطلاعات مربوط به گزارشات انحصاری، مذاکرات و جلسات هستند. بدست آوردن این اطلاعات بسیار دشوار است. به دلیل اینکه این اطلاعات حاوی راهبردهای مهاجمان هستند بازه زمانی کاربرد آن‌ها بلند مدت (چند سال) است.ازجمله مزایای بهره گیری از هوش امنیتی راهبردی در سازمان عبارتند از: کاهش تهدیدات، کاهش سطح عدم انطباق، تسهیل تصمیم‌گیری‌های امنیتی، خودکار نمودن فرآیندهای امنیتی و هدف هوش امنیتی در مقابله با جنگ ترکیبی می توان نام برد.

روش پژوهش

تحقیق حاضر به لحاظ هدف، کاربردی، به لحاظ روش استنتاج، توصیفی و به لحاظ ماهیت داده‌ها، کیفی و کمی است. تحقیق حاضر از فرآیندی سه مرحله‌ای تبعیت می‌کند:

الف) بخش کیفی: در وهله نخست، پس از مطالعه کتابخانه‌ای، به جهت شناسایی الزامات هوش امنیتی و همچنین راهبردهای بهبود آن در جنگ ترکیبی، از مصاحبه نیمه ساختاریافته و سوالات زیر استفاده گردید:

الزامات و راهبردهای هوش امنیتی در جنگ ترکیبی کدامند؟

چه راهبردهایی جهت بهبود هوش امنیتی در جنگ ترکیبی می‌توان اتخاذ نمود؟

همچنین، تحلیل محتوای مصاحبه‌ها با استفاده از روش گرندد تئوری و کدگذاری در دو سطح باز و محوری، انجام شد. جامعه آماری این تحقیق را اعضاء هیئت علمی در مراکز علمی مرتبط با امنیت و مدیران و کارشناسان فعال در زمینه امنیت و اطلاعات در سازمانهای نظامی و انتظامی کشور، تشکیل دادند. با توجه به حاکمیت رویکرد کیفی در این بخش، از روش نمونه گیری نظری که یکی از روش‌های نمونه‌گیری هدفمند متوالی یا متواتر است، استفاده شد. در نمونه گیری نظری، نمونه‌ها به شکلی انتخاب می‌شوند که به خلق تئوری کمک کنند. در این روش به جای انتخاب یک نمونه ثابت حجم نمونه آنقدرافزایش می‌یابد تا زمانیکه دیگر کافی باشد (اشباع نظری) (بازرگان‌هرندی و دیگران، ۱۳۹۷). بر همین اساس، بعد از انجامِ نه مصاحبه، دیده شد که عوامل اصلی و فرعی در مصاحبه‌ها تکرار شده و پاسخ‌ها از روندی تکراری تبعییت می‌کنند اما برای اطمینان بیشتر،علاوه برتحلیل پنج منبع بصورت کتابخانه ای، سه مصاحبه دیگر نیز انجام شد و نمونه با ۱۲ نفر مورد تأیید قرار گرفت و به فرایند مصاحبه پایان داده شد و پژوهشگر به اشباع نظری رسید. پس از پیاده سازی مصاحبه‌ها، یافته‌های تحقیق به صورت متن درآمده، و در نرم افزار MAXQDA کدگذاری و مقوله بندی شده و اقدام به تحلیل آن‌ها گردید.

ب)بخش کمی اول: در این مرحله، به منظور تعیین درجه اهمیت الزامات هوش امنیتی از روش آنتروپی شانون[1] استفاده شده است. در اکثر مسائل تصمیم‌گیری چندمعیاره دانستن وزن عناصر بسیار مهم است. تکنیک آنتروپی شانون یکی از روش‌هایی است که برای تعیین وزن عناصر مورد استفاده قرار می‌گیرد. در این تکنیک وزن عناصر براساس میزان پراکندگی مقادیر عنصر مورد تعیین می‌شود. روش مذکور اولین بار توسط استفان بولتزمن مطرح و نهایتاً توسط شانن[2](۱۹۴۸) به صورت کمی ارائه شد. آنتروپی در حقیقت بیانگر آن است که چگونه از بین عوامل مؤثر یک هدف، می‌توان مهم‌ترین عوامل را تخمین زد یا به عبارتی متغیرهایی که بیشترین تأثیر را در رخ داد یک واقعیت دارند برای ما مشخص می‌نماید.

ج) بخش کمی دوم: در این مرحله، به منظور رتبه بندی راهبردهای بهبود هوش امنیتی در در جنگ ترکیبی از روش ماباک (MABAC)، استفاده شده است. روش ماباک (MABAC) از جدیدترین تکنیک‌های تصمیم گیری چند معیاره است که جهت رتبه بندی گزینه‌ها در مدل‌های تصمیم گیری چند معیاره استفاده می‌شود این روش اولین بار توسط پاموکار و سیروویچ[3](۲۰۱۵) ارائه شد.

---

1. Shanon Entropy
2. Shannon
3. Pamucar & cirovic

مزایای استفاده از روش MABAC به شرح زیر است: (۱) دارای دستگاه ریاضی ساده و نتایج پایدار است. (۲) نتایج کاملی را می‌توان به راحتی با این روش بدست آورد زیرا ارزش‌های احتمالی سود و ضرر را در نظر می‌گیرد. و (۳) ترکیب این روش با رویکردهای دیگر امکان پذیر است. از این رو، روش MABACاین توانایی را دارد که نیازهای یک ابزار اولویت بندی معتبر را برآورده سازد.

۵. یافته‌های تحقیق

مرحله اول: شناسایی الزامات و راهبردهای امنیتی هوش امنیتی در مقابله با جنگ ترکیبی

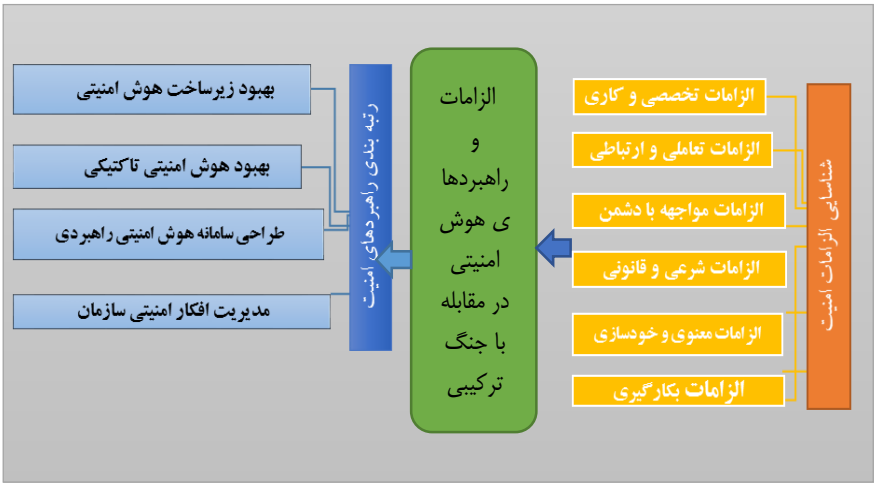
در این بخش از تحقیق، نتایج حاصل از کدگذاری اولیه یا کدگذاری باز و محوری ارائه می‌شود. لازم به ذکر است که جهت اعتبارسنجی نتایج بخش کیفی در این مطالعه، از روش کنترل اعضا (محققین یافته‌های خود را با چهار نفر از افراد مطلع تحت بررسی کنترل نموده و تفاسیر پژوهشگر به تأیید رسیده است)، استفاده شده است. جهت اختصار خلاصه تحلیل مصاحبه‌ها در جدول (۱) بیان شده است:

جدول (۴): کدگذاری مصاحبه‌ها و استخراج الزامات وراهبردهای هوش امنیتی در مقابله با جنگ ترکیبی

مقوله‌ها	شاخص‌ها	علامت	مفاهیم (اعداد داخل پرانتز نشان‌دهنده شماره مصاحبه‌شونده است)
الزامات امنیتی هوش امنیتی در مقابله با جنگ ترکیبی	الزامات تخصصی امنیت	C1	ارتقاء آموزش‌های تخصصی فناوری اطلاعات (۳)، بومی‌سازی دانش ساخت ابزارهای فنی در داخل (۴)، آموزش تخصصی امنیتی وآگاه سازی حفاظتی (۷)، بکارگیری عوامل اجرایی متخصص (۱۱)
	الزامات تعاملی امنیت	C2	انتقال تجربیات موفق به همکاران (۲)، تعامل دستگاه‌های اطلاعاتی (۷)، گزارش دهی اطلاعاتی (۱۰)، عدم پنهان کاری مفرط در مناسبات حساس سازمان (۱۱)، رعایت سلسله مراتب سازمانی (۱۲)
	الزامات بکارگیری امنیت	C3	مشورت امنیتی در قراردادها و... (۱)، پیش‌بینی آسیب و تهدیدات امنیتی (۳)، احصاء سیاست امنیتی در خط‌مشی گذاری‌ها (۶)، مسئولیت پذیری امنیتی (۸)، ضرورت نظارت و کنترل امنیتی (۹)، ایجاد بازدارندگی مؤثر امنیتی (۱۱)
	الزامات مواجهه با دشمن	C4	هوشیاری درمقابل تهدیدات دشمن (۳)، رویکرد تهاجم اطلاعاتی در مقابل دشمن (۴)، بی اعتبارساختن دشمن (۵)، شناخت راهکارهای دشمن (۷)، ضرورت شناخت اطلاعاتی دشمن (۱۰)، شناخت ظرفیت امنیتی دشمن (۱۲)

	الزامات شرعی و قانونی	C5	رعایت موازین شرعی (۱)، توجه به انضباط معنوی (۴)، تعهد به ارزشهای اخلاقی و قانونی (۵)، پیروی از ولایت فقیه (۹)
	الزامات فردی و خودسازی	C6	مراقبت از نفس (۲)، اتصال به مبدأ هستی (۵)، قابلیت مواجهه با مشکلات و ناملایمات (۶)، مستقل بودن (شهامت) (۱۲)
راهبردهای امنیتی هوش امنیتی در مقابله با جنگ ترکیبی	مدیریت افکار امنیتی سازمان	A1	اعتمادسازی کارکنان (۳)، قدرت اقناع سازی مدیران (۵)، شناخت نگرش مخاطبین (۷)، رفع تضادهای امنیتی سازمانی (۸)، اثرگذاری امنیتی در حفاظت روانی کارکنان (۹)، آگاه سازی حفاظتی در مجموعه سازمان (۱۰)
	طراحی سامانه هوش امنیتی راهبردی	A2	طراحی نرم‌افزارهای بومی و سطح بالای امنیتی در سازمان (۱)، طراحی سیستم بهنگام شناسایی رخداد سایبری (۶)، طراحی راهکار مقابله با نفوذ در سازمان‌ها (۹)، طراحی سیستم پیش‌بینی تغییرمخاطرات (۱۱)
	بهبود هوش امنیتی تاکتیکی	A3	بهبود مدیریت شبکه (۷)، ایجاد نوآوری در تاکتیک‌های امنیتی (۹)، ارتقا دانش مدیران امنیتی (۱۱)، زمان شناسی بحران سازمانی (۱۲)
	بهبود زیرساخت هوش امنیتی	A4	ارتقا سخت‌افزاری ابزارهای مقابله با نفوذ (۱)، بهینه سازی سخت‌افزاری و نرم‌افزاری مقابله با بدافزارهای بومی (۶)، بهبود زیرساخت سیستم پایش شبکه (۸)، ارتقا و بهبود سرورهای کنترل (۱۰)، ایجاد مرکز عملیات یکپارچه (۱۱)

جهت پیاده سازی واستقرار راهبردهای امنیت مدل هوش امنیتی در مقابله با جنگ ترکیبی ، برابرجدول شماره(۱) پس از شناسایی الزامات امنیت شامل: تخصصی ،تعاملی ،بکارگیری ،فردی و خودسازی،مواجهه با دشمن ، شرعی ، قانونی و همچنین راهبردهای بهبود آن درساختار حاکمیت شامل بهبود زیرساخت، بهبود هوش امنیتی تاکتیکی،طراحی سامانه راهبردی امنیت ومدیریت افکار امنیتی به ترتیب رتبه بندی (مقوله‌ها)، تعیین گردید، مدل مفهومی آن درقالب شکل(۱) ترسیم می‌گردد.



شکل (۵): مدل مفهومی الزامات وراهبردهای هوش امنیتی در مقابله با جنگ ترکیبی

مرحله دوم: تعیین درجه اهمیت الزامات امنیتی هوش امنیتی در مقابله جنگ ترکیبی

همانگونه که بیان شد جهت تعیین درجه اهمیت الزامات هوش امنیتی در مقابله با جنگ ترکیبی ، از روش آنتروپی شانون استفاده شد. بر همین اساس پس از کسب نظر خبرگان(۱۲ نفر) وتحلیل محتوا پنج منبع بصورت کتابخانه ای به وسیله پرسشنامه و جمع‌بندی نظرات؛ گام‌های زیر جهت تجزیه و تحلیل داده‌ها انجام شد:

گام اول، تشکیل ماتریس تصمیم: در این پژوهش از طیف لیکرت پنج درجه‌ای (خیلی کم، کم، متوسط، زیاد، خیلی زیاد)، برای ارزیابی استفاده شد. با توجه به میانگین نظر خبرگان، ماتریس تصمیم تشکیل گردید. برای تشکیل این ماتریس کافیست اگر معیارها کیفی هستند از عبارات کلامی ارزیابی هر گزینه را نسبت به هر معیار به دست آورد و اگر معیارها کمی هستند عدد واقعی آن ارزیابی را قرار داد. در ماتریس تصمیم پژوهش حاضر، معیارها؛ الزامات هوش امنیتی و گزینه‌ها؛ راهبردهای بهبود هوش امنیتی در مقابله با جنگ ترکیبی ، هستند.

گام دوم، نرمالایز ماتریس تصمیم: در این گام، ماتریس تصمیم را نرمال می‌کنیم و هر درایه نرمال شده را pij می‌نامیم. نرمال شدن به این صورت است که درایه هر ستون را بر مجموع ستون تقسیم می‌کنیم. نتایج محاسبات گام اول و دوم در جدول (۲)، نشان داده شده است:

جدول (۶): ماتریس تصمیم گیری نرمال شده (بی مقیاس شده)

C6	C5	C4	C3	C2	C1	
0.260	0.280	0.216	0.244	0.230	0.194	A1
0.225	0.219	0.237	0.229	0.213	0.217	A2
0.265	0.250	0.253	0.256	0.255	0.277	A3
0.249	0.250	0.294	0.270	0.301	0.312	A4

گام سوم، محاسبه آنتروپی هر شاخص: آنتروپی Ej به صورت زیر محاسبه می‌گردد و k به عنوان مقدار ثابت مقدار Ej را بین ۰ و ۱ نگه می‌دارد.

$$E_j = -k\sum_{i=1}^{m} P_{ij} \times Ln\, P_{ij} \;\; , k = \frac{1}{\ln m} \;\; , \;\; i = 1.2.\ldots.m$$

جدول ۷- محاسبه $(-\boldsymbol{kP_{ij}} \times \boldsymbol{Ln\, P_{ij}})$

C6	C5	C4	C3	C2	C1	
0.253	0.257	0.239	0.248	0.244	0.229	A1
0.242	0.240	0.246	0.243	0.238	0.239	A2
0.254	0.250	0.251	0.252	0.251	0.257	A3
0.250	0.250	0.260	0.255	0.261	0.262	A4

لازم به ذکر است که افزایش در آنتروپی شانون باعث افزایش عدم اطمینان و کاهش اطلاعات در مورد دانش متغیر تصادفی می‌شود. جنبه جالب دیگر آنتروپی شانون ویژگی حداکثر آنتروپی آن برای توزیع یکنواخت است.

گام چهارم، محاسبه فاصله هر شاخص از آنتروپی آن (تعیین درجه انحراف): در ادامه مقدار dj (درجه انحراف) محاسبه می‌شود (dj=1-Ej) که بیان می‌کند شاخص مربوطه (dj) چه میزان اطلاعات مفید برای تصمیم گیری در اختیار تصمیم گیرنده قرار می‌دهد. هر چه مقادیر اندازه گیری شده شاخصی به هم نزدیک باشند نشان دهنده آنست که گزینه‌های رقیب از نظر آن شاخص تفاوت چندانی با یکدیگر ندارند. لذا نقش آن شاخص در تصمیم گیری باید به همان اندازه کاهش یابد.

گام پنجم، تعیین وزن هر شاخص: سپس مقدار وزن Wj محاسبه می‌گردد. در واقع وزن معیار برابر با هر dj تقسیم بر مجموعdj ها (wj=dj/∑dj)، می‌باشد. نتایج محاسبات گام چهارم و پنجم در جدول (۴)، نشان داده شده است:

جدول ۸- محاسبه آنتروپی هر شاخص، درجه انحراف، وزن و رتبه هر شاخص

شاخص‌ها	C1	C2	C3	C4	C5	C6
آنتروپی هر شاخص (Ej)	0.987	0.994	0.999	0.995	0.997	0.999
درجه انحراف هر شاخص (Dj)	0.013	0.006	0.001	0.005	0.003	0.001
وزن هر شاخص (Wj)	0.439	0.213	0.047	0.161	0.093	0.047
رتبه هر شاخص	1	2	6	3	4	5

با توجه به نتایج این بخش(جدول ۴)، الزامات تخصصی هوش امنیتی (C1)، الزامات تعاملی هوش امنیتی(C2)، الزامات مواجهه با دشمن(C4)، الزامات شرعی و قانونی(C5)، الزامات فردی و خودسازی (C6) و الزامات بکارگیری هوش امنیتی(C3)، به ترتیب بالاترین درجه اهمیت را در میان الزامات هوش امنیتی درمقابله با جنگ ترکیبی را، کسب کردند.

مرحله سوم: رتبه بندی راهبردهای بهبود هوش امنیتی در مقابله با جنگ ترکیبی

در این بخش از تحقیق، جهت رتبه بندی راهبردهای بهبود هوش امنیتی در مقابله با جنگ ترکیبی ، از روش ما باک استفاده شد. بر همین اساس پس از کسب نظر خبرگان(۱۲ نفر) به وسیله پرسشنامه و جمع‌بندی نظرات؛ گام‌های زیر جهت تجزیه و تحلیل داده‌ها انجام شد:

گام اوّل، تشکیل ماتریس اولیه تصمیم(X): در این گام فرض می‌شود تعداد m گزینه و n معیار موجود است. هر یک از گزینه‌ها به شکل برداری و به صورت Aij= (xi1,xi2,…,xin) نمایش داده می‌شوند که xij وضعیت گزینه i ام در معیار j ام را مشخص می‌نماید. بر این اساس ماتریس تصمیم اولیه همان ماتریس مرحله قبل (آنتروپی شانون)، می‌باشد. همچنین xij درایه‌های ماتریس اولیه تصمیم (X) بوده و xi- و+xi به صورت زیر تعریف می‌شوند:

$x_i^+ = \max(x_1. x_2. \dots x_m)$: نشان دهنده بیشترین مقداری است که در یک معیار مشخص، در میان گزینه‌ها مشاهده شده است.

$x_i^- = \min(x_1. x_2. \dots x_m)$: نشان دهنده کمترین مقداری است که در یک معیار مشخص، در میان گزینه‌ها مشاهده شده است.

نتایج محاسبات گام اول در جدول (۵)، نشان داده شده است:

جدول ۹- ماتریس اولیه (میانگین نظر پاسخ دهندگان)

	C1	C2	C3	C4	C5	C6
A1	2.262	3.033	3.357	2.952	3.595	3.405
A2	2.533	2.810	3.143	3.238	2.810	2.952
A3	3.238	3.357	3.524	3.452	3.214	3.476
A4	3.643	3.967	3.714	4.024	3.214	3.262
X+	3.643	3.967	3.714	4.024	3.595	3.476
X-	2.262	2.810	3.143	2.952	2.810	2.952
W	0.439	0.213	0.047	0.161	0.093	0.047

گام دوم، نرمال کردن درایه‌های ماتریس تصمیم اولیه (N): به دلیل آنکه ممکن است جنس هر یک از معیارها متفاوت باشند، در گام دوم ماتریس تصمیم نرمال شده تا اثر مقیاس متفاوت معیارها خنثی شود. به‌منظور انجام این کار و با توجه به جنس هر معیار، از رابطه$n_{ij} = \frac{x_{ij}-x_i^-}{x_i^+-x_i^-}$ برای نرمال سازی معیارهای مثبت و ازرابطه $n_{ij} = \frac{x_{ij}-x_i^+}{x_i^--x_i^+}$ برای نرمال سازی معیارهای منفی استفاده می‌شود. لازم به ذکر است که در این تحقیق شاخص‌های چالش بین بخشی (C7) و بارکاری (C11)، به عنوان معیارهای منفی در نظر گرفته شدند. نتایج این گام در جدول (۶)، نشان داده شده است:

جدول ۱۰-نرمالسازی ماتریس اولیه (N)

	C1	C2	C3	C4	C5	C6
A1	0.000	0.559	0.793	0.500	0.966	0.828
A2	0.197	0.397	0.638	0.707	0.397	0.500
A3	0.707	0.793	0.914	0.862	0.690	0.879
A4	1.000	1.234	1.052	1.276	0.690	0.724

گام سوم: تشکیل ماتریس تصمیم نرمال موزون (V): از آنجا که معیارها دارای وزن متفاوتی در فرایند ارزیابی هستند؛ در این گام می‌بایست درایه‌های ماتریس نرمال موزون بر اساس رابطه ($v_{ij} = w_i(n_{ij}+1)$) محاسبه شوند. در این رابطه nij درایه‌های ماتریس نرمال (N) و wi وزن معیار i ام می‌باشد. همچنین vij درایه‌های ماتریس موزون V را تشکیل می‌دهد. این ماتریس به شکل زیر تعریف می‌شود:

جدول ۱۱-تشکیل ماتریس موزون (V)

	C1	C2	C3	C4	C5	C6
A1	0.439	0.332	0.084	0.242	0.183	0.087
A2	0.525	0.297	0.076	0.275	0.130	0.071
A3	0.749	0.381	0.089	0.300	0.158	0.089
A4	0.877	0.475	0.096	0.367	0.158	0.082

گام چهارم، مشخص کردن ماتریس مرز تخمین ناحیه (G): مرز تخمین ناحیه برای هر معیار به شکل رابطه $g_i = \left(\prod_{j=1}^{m} v_{ij}\right)^{1/m}$، محاسبه می‌شود. بعد از محاسبه gi برای هر معیار، ماتریس مرز تخمین ناحیه که با G نشان داده می‌شود، تشکیل می‌گردد که در جدول (۸)، نشان داده شده است:

جدول ۱۲-ماتریس مرز تخمین ناحیه (میانگین هندسی هر ستون از ماتریس موزون)

	C1	C2	C3	C4	C5	C6
gi	3.789	1.741	0.225	1.268	0.522	0.210

گام پنجم، محاسبه فاصله گزینه‌ها از مرز تخمین ناحیه (Q): فاصله گزینه‌ها از مرز تخمین ناحیه مطابق رابطه $Q = V - G$، برابر اختلاف میان درایه‌های ماتریس وزن دار (V) و مقدار مرز تخمین ناحیه (G) تعیین می‌شود. پس از مشخص شدن مقدار ماتریس Q، می‌توان با تعریف بردار تخمین مساحت (G)، حد بالایی مساحت (+G) و حد پایین مساحت (-G) وضعیت هر گزینه را مشخص نمود. بر این اساس، گزینه Ai متعلق به اجتماع مجموعه مذکور می‌باشد. نواحی مذکور در شکل ۱ نشان داده شده‌اند. در این تعریف، حد بالای تخمین مساحت (+G)، منطقه‌ای است که گزینه ایده آل (+A) در آن منطقه حضور داشته و حد پایین تخمین مساحت (-G) منطقه‌ای است که گزینه ضد ایده آل (-A) در آنجا وجود دارد. میزان تعلّق گزینه Ai به اجتماع مذکور، بر اساس رابطه زیر به دست می‌آید.

$$A_i \in \begin{cases} G^+ q_{ij} > 0 \\ G q_{ij} = 0 \\ G^- q_{ij} < 0 \end{cases}$$

بر مبنای منطق روش ماباک برای اینکه گزینه Ai بهترین گزینه در مجموعه گزینه‌ها باشد؛ لازم است تا نسبت به دیگر گزینه‌ها به حد بالای تخمین منطقه‌ای (+G) نزدیک‌تر باشد. به عبارت دیگر، اگر مقدار

qij>۰ باشد، بنابراین گزینه Ai نزدیک یا برابر گزینه ایده آل خواهد بود. همین مساله به صورت معکوس و برای شرایط qij<۰ نیز وجود دارد. به گونه‌ای که اگر qij<۰ باشد، بنابراین گزینه Ai نزدیک یا برابر گزینه ضد ایده آل می‌باشد. نتایج این گام در جدول (۹)، نشان داده شده است:

جدول ۱۳-محاسبه فاصله گزینه‌ها از مرز تخمین (Q)

	C1	C2	C3	C4	C5	C6
A1	-3.351	-1.409	-0.142	-1.026	-0.339	-0.124
A2	-3.265	-1.443	-0.149	-0.992	-0.392	-0.139
A3	-3.041	-1.359	-0.136	-0.967	-0.365	-0.121
A4	-2.912	-1.265	-0.130	-0.901	-0.365	-0.129

گام ششم رتبه بندی گزینه‌ها: در آخرین گام از روش ماباک، مقدار توابع معیارها بر اساس مجموع فواصل گزینه‌ها از بردار تخمین مساحت (qi) برای هر کدام، مطابق رابطه $S_i = \sum_{j=1}^{n} q_{ij}$، محاسبه می‌شود. با محاسبه مجموع درایه‌های ماتریس Q به صورت سطری، مقدار نهایی توابع معیار برای هر گزینه مشخص شده و مبنای رتبه‌بندی گزینه‌ها قرار می‌گیرد. در پایان، رتبه بندی الزامات و راهبردهای بهبود هوش امنیتی در جنگ ترکیبی، با روش ماباک، انجام پذیرفت ودر قالب جدول زیر می آید.

جدول ۱۴-رتبه بندی گرینه‌ها

رتبه	گزینه‌ها		si
۱	بهبود زیرساخت هوش امنیتی	A4	-5.701
۲	بهبود هوش امنیتی تاکتیکی	A3	-5.989
۳	طراحی سامانه هوش امنیتی راهبردی	A2	-6.380
۴	مدیریت افکار امنیتی سازمان	A1	-6.390

با توجه به سوال تحقیق مبنی بر اینکه الزامات هوش امنیتی در مقابله با جنگ ترکیبی کدامند یافته‌های تحقیق نشان می دهد الزامات تخصصی امنیتی، الزامات تعاملی امنیتی، الزامات مواجهه با دشمن، الزامات شرعی و قانونی، الزامات فردی و خودسازی و الزامات بکارگیری هوش امنیتی به ترتیب بالاترین درجه اهمیت را در میان الزامات هوش امنیتی در مقابله با جنگ ترکیبی ، کسب کرده‌اند به بیان دیگر جهت استقرار هوش امنیت در ساختارها ومتولیان امنیت باید به الزامات تخصصی از قبیل ارتقاء

آموزش‌های تخصصی فناوری اطلاعات، بومی‌سازی دانش ساخت ابزارهای فنی در داخل ، آموزش تخصصی امنیتی وآگاه سازی حفاظتی ، بکارگیری عوامل اجرایی متخصص توجه گردد.

همچنین بر اساس سوال تحقیق مبنی براینکه چه راهبردهایی جهت بهبود هوش امنیتی در مقابله با جنگ ترکیبی می‌توان اتخاذ نمود، یافته‌های تحقیق نشان می دهد بهبود زیرساخت هوش امنیتی، بهبود هوش امنیتی تاکتیکی، طراحی سیستم هوش امنیتی راهبردی و مدیریت افکار امنیتی سازمان، به ترتیب بالاترین رتبه را در میان راهبردهای بهبود هوش امنیتی در مقابله با جنگ ترکیبی ، کسب کردند.یعنی اینکه جهت مشخص نمودن راهبرد پیاده سازی الزامات هوش امنیتی در مقابله با جنگ ترکیبی باید بهبود زیرساخت هوش امنیتی از قبیل ارتقا سخت‌افزاری ابزارهای مقابله با نفوذ، بهینه سازی سخت‌افزاری و نرم‌افزاری مقابله با بدافزارهای بومی ، بهبود زیرساخت سیستم پایش شبکه، ارتقا و بهبود سرورهای کنترل ،و ایجاد مرکز عملیات یکپارچه دراولویت قرارگیرد.

نتیجه‌گیری و پیشنهادات

امنیت از نیازهای فطری بشر و گرایش به امنیت پایدار، یکی از نیازهای عالی انسانی است که تحقق آن نیازمند محیطی است که بتواند به دور از فشارها گروهی و در مسیر رشد قرار گیرد؛ بنابراین آسودگی زیستن به ساز و کارهای متعدد و گوناگونی نیاز دارد که سرلوحه آنها امنیت است. امنیت در گذشته در پرتو قدرت نظامی تحقق پیدا می‌کرد ولی امروزه با تحولی که در فناوری ارتباطات و اطلاعات به وجود آمده؛ در ابعاد گسترده‌تری اهمیت یافته و احساس ضرورت آن نه تنها در ابعاد مادی، بلکه در ابعاد معنوی نیز احساس می‌شود. نیازمندی‌های نوین بشری از یک‌سو و دشواری و چالش‌های نوپدید(جنگ ترکیبی) از سوی دیگر منجر به گسترده شدن مفهوم امنیت در عصر حاضر شده است.همانطورکه در جهان واقعی، انسان‌های موفق افرادی هستند که استعدادی سرشار داشته و از هوش بالایی برخوردار می‌باشند، قطعاً در سازمان‌ها نیز چنین است؛ به‌خصوص در زمان فعلی هرچه زمان به جلو حرکت می‌کند، به علت پیشرفت علوم و فنون و به وجود آمدن اقتضائات جدید، سازمان‌ها نیز چالشی‌تر و مدیریت آن‌ها سخت‌تر می‌شود. لذا، ادامه حیات سازمان‌ها متأثر از قابلیت سازگاری آن‌ها برای تبعیت از تغییرات است. در این بین، هوش امنیتی به دنبال مدیریت همه جانبه اطلاعات امنیتی در مقابله با جنگ ترکیبی دشمن که مورد تاکید مقام معظم رهبری بوده و بارها به آنها اشاره فرموده اند. می‌باشد. الزامات وراهبردهای هوش امنیتی کمک می کند درمقابله با جنگ ترکیبی در واقع با بکارگیری مهارت‌های لازم در جهت جمع آوری، یکپارچه سازی و تحلیل تمام اطلاعات مذکور به دنبال مدیریت و در نهایت بهینه سازی و افزایش هوشمندی سازمانی ومدیران و مجریان حاکمیت در امور امنیتی است.

با توجه به یافته‌های تحقیق راهکاری زیر جهت مقابله با جنگ ترکیبی دشمن پیشنهاد می گردد:

۱. تحقق منویات مقام معظم رهبری(مدالضله العالی) در مقابله با جنگ ترکیبی
۲. نهادینه سازی فرهنگ امنیتی مقابله با جنگ ترکیبی؛
۳. با ارتقا و بهینه‌سازی سخت‌افزاری و نرم‌افزاری ابزارهای جهت مقابله با جنگ ترکیبی دشمن، همانند بهبود زیرساخت سیستم پایش شبکه، ارتقا و بهبود سرورهای کنترل و همچنین ایجاد مرکز عملیات یکپارچه؛
۴. فرهنگ سازی هوش امنیتی در بین مدیران و متولیان و...جهت مقابله با تهدیدات و آسیب‌های سازمانی از طریق مقابله با جنگ ترکیبی؛
۵. استقرارسامانه ارزیابی امنیتی در سازمان‌ها جهت تعیین میزان خسارات شکست امنیتی وعملکرد امنیتی مدیران ارشد حاکمیت در سازمان‌ها؛

۶. بهبود مدیریت شبکه، ایجاد نوآوری در تاکتیک‌های امنیتی و ارتقا دانش مدیران امنیتی درمقابله با جنگ ترکیبی، مد نظر قرار دهند؛

۷. جهت مقابله با جنگ ترکیبی دشمن با انجام سلسله اقداماتی نظیر اعتمادسازی درکارکنان، شناخت نگرش‌های متفاوت مخاطبین، رفع تضادهای امنیتی سازمانی ، اثرگذاری امنیتی در حفاظت روانی کارکنان و آگاه سازی حفاظتی در مجموعه سازمان، مدیریت افکار امنیتی را در سازمان، نهادینه کنند.

منابع

۱ . اکبرزاده، نسرین. (1383). هوش هیجاني از دیدگاه سالوي و دیگران. تهران: انتشارات فارابي.

۲ . بازرگان‌هرندی، عباس؛ حجازی، الهه؛ و سرمد، زهره. (۱۳۹۷). روش‌های تحقیق در علوم رفتاری.انتشارات آگه.

۳ . خدادادی، مجتبی؛ و حسنپور، علی. (۱۳۹۲). نقش هوش هیجانی در توانمندی مدیران امنیتی. پژوهش‌های حفاظتی و امنیتی، ۵(۲)، ۹۵-۱۱۰.

۴ . رضایت، غلامحسین؛ و مرادیان، فیض اله. (۱۳۹۵). ارائه الگوی راهبردی حفاظت اطلاعات اسلامی. دانشگاه عالی دفاع ملی (دانشکده امنیت ملی)، ۶(۲۲)، ۶۹-۹۴.

۵ . سیف، علی اکبر. (۱۳۹۸). روانشناسی پرورشی نوین: روانشناسی یادگیری و آموزش. دوران.

۶ . . شیدائیان، حسین.(۱۳۸۸) امنیت ملي از منظر امام و مقام معظم رهبري فصلنامه حصو ن، شماره۱۹

۷ . عاطف،رضا۱۳۷۸«بررسي اطلاعات»تهران دانشکده وپژوهشکده اطلاعات وامنیت

۸ . قربانی زواره، محمد حسین (۱۳۹۸)، جنگ ترکیبی (چگونگی مناقشات در قرن معاصر)، انتشارات دافوس آجا

۹ . قریب،حسین"جهانی شدن وچالش‌های امنیتی ایران"۱۳۸۰اطلاعات سیاسی-اقتصادی مردادوشهریور

۱۰ . کاتوزیان، ناصر، مقدمه علم حقوق، چاپ هجدهم، تهران، بهمن، ۱۳۷۳.

۱۱ . کوریبکو، اندرو (۱۴۰۰)، جنگ‌های ترکیبی (استراتژی کلان غیر مستقیم ایالات متحده آمریکا علیه دولت‌های مستقل و ملی) ترجمه سبحان محمدی، انتشارات آرون، چاپ صدف

۱۲ . عصاریان حسین ۱۳۸۳ ملی اطلاعات مقاله چاپ شده دانشکده علوم و فنون فناوری آبی تهران

۱۳ . عمادی ابوالفضل،۱۳۹۸،"مدیریت بحران" انتشارات مرکز آموزش

14 . Crump, Justin. (2015). *Corporate security intelligence and strategic decision making*. Crc press.
15 . Gardner, Howard. (2006). *Intelligence reframed: Multiple intelligences for the new millennium*. Basic Books.
16 . Gardner, Howard; & Hatch, Thomas. (1990). Multiple Intelligences Go to School: Educational Implications of the Theory of Multiple Intelligences. Technical Report No. 4.
17 . Gardner, Hall. (2015) Hybrid Warfare: Iranian and Russian Versions of "Little Green
18 . Men" and Contemporary Conflict. NATO Defense College, Rome.
19 . Kaiser, Robert. (2015). The birth of cyberwar. *Political Geography*, *46*, 11-20.
20 . Manogaran, Gunasekaran; Thota, Chandu; Lopez, Daphne; & Sundarasekar, Revathi. (2017). Big data security intelligence for healthcare industry 4.0. In *Cybersecurity for Industry 4.0* (pp. 103-126). Springer.
21 . Pamucar, Dragan; & cirovic, Goran. (2015). The selection of transport and handling resources in logistics centers using Multi-Attributive Border Approximation area Comparison (MABAC). *Expert Systems with Applications*, *42*(6), 3016-3028. https://doi.org/10.1016/j.eswa.2014.11.057
22 . Pham, Hiep Cong; Brennan, Linda; & Furnell, Steven. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications*, *46*, 96-107.
23 . Pirc, John; DeSanto, David; Davison, Iain; & Gragido, Will. (2016a). 3 - Security Intelligence. In J. Pirc, D. DeSanto, I. Davison, & W. Gragido (eds.), (J. Pirc, D. DeSanto, I. Davison, & W. Gragido, eds.), *Threat Forecasting* (pp. 29-45). Syngress.
24 . Pirc, John; DeSanto, David; Davison, Iain; & Gragido, Will. (2016b). *Threat forecasting: Leveraging big data for predictive analysis*. Syngress.
25 . Sallos, Mark Paul; Garcia-Perez, Alexeis; Bedford, Denise; & Orlando, Beatrice. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*.
26 . Samonas, Spyridon; Dhillon, Gurpreet; & Almusharraf, Ahlam. (2020). Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management*, *50*, 144-154.
27 . Shannon, Claude E. (1948). A mathematical theory of communication. *The Bell system technical journal*, *27*(3), 379-423.

Sternberg, Robert J; Grigorenko, Elena L; & Bundy, Donald A. (2001). The Predictive Value of IQ. *Merrill-Palmer Quarterly*, *47*(1), 1-1.